MultiNet for OpenVMS Installation and Introduction

Part Number: N-5004-43-NN-A

August 2000

This guide describes how to install Process Software's MultiNet for OpenVMS and its layered products on (or remove them from) systems running the OpenVMS VAX and OpenVMS Alpha Operating Systems. An overview of MultiNet and TCP/IP concepts follows the installation chapters.

Revision/Update: This guide replaces the *MultiNet Installation and Introduction*, Version V4.2

Operating System/Version: VAX/VMS V5.5-2 or later, OpenVMS VAX V6.0 or later, or OpenVMS Alpha V6.1 or later

Software Version: MultiNet V4.3

PERFORMANCE OF THIS SOFTWARE.

Portions Copyright © 1995 by International Business Machines, Inc.
International Business Machines, Inc. (hereinafter called IBM) grants permission under its copyrights to use, copy, modify, and distribute this Software with or without fee, provided that the above copyright notice and all paragraphs of this notice appear in all copies, and that the name of IBM not be used in connection with the marketing of any product incorporating the Software or modifications thereof, without specific, written prior permission. To the extent it has a right to do so, IBM grants an immunity from suit under its patents, if any, for the use, sale or manufacture of products to the extent that such products are used for performing Domain Name System dynamic updates in TCP/IP networks by means of the Software. No immunity is granted for any product per se or for any other function of any product. THE SOFTWARE IS PROVIDED "AS IS", AND IBM DISCLAIMS ALL WARRANTIES, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL IBM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE, EVEN IF IBM IS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

Portions Copyright © 1995, 1996, 1997, 1998, 1999, 2000 by Internet Software Consortium. All Rights Reserved. Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies. THE SOFTWARE IS PROVIDED "AS IS" AND INTERNET SOFTWARE CONSORTIUM DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL INTERNET SOFTWARE CONSORTIUM BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.
Copyright (c) 1996-2000 Internet Software Consortium.
Use is subject to license terms which appear in the file named ISC-LICENSE that should have accompanied this file when you received it. If a file named ISC-LICENSE did not accompany this file, or you are not sure the one you have is correct, you may obtain an applicable copy of the license at: http://www.isc.org/isc-license-1.0.html. This file is part of the ISC DHCP distribution. The documentation associated with this file is listed in the file DOCUMENTATION, included in the top-level directory of this release. Support and other services are available for ISC products - see http://www.isc.org for more information.
ISC LICENSE, Version 1.0
1. This license covers any file containing a statement following its copyright message indicating that it is covered by this license. It also covers any text or binary file, executable, electronic or printed image that is derived from a file that is covered by this license, or is a modified version of a file covered by this license, whether such works exist now or in the future. Hereafter, such works will be referred to as "works covered by this license," or "covered works."
2. Each source file covered by this license contains a sequence of text starting with the copyright message and ending with "Support and other services are available for ISC products - see http://www.isc.org for more information." This will hereafter be referred to as the file's Bootstrap License.
3. If you take significant portions of any source file covered by this license and include those portions in some other file, then you must also copy the Bootstrap License into that other file, and that file becomes a covered file. You may make a good-faith judgement as to where in this file the bootstrap license should appear.
4. The acronym "ISC", when used in this license or generally in the context of works covered by this license, is an abbreviation for the words "Internet Software Consortium."
5. A distribution, as referred to hereafter, is any file, collection of printed text, CD ROM, boxed set, or other collection, physical or electronic, which can be distributed as a single object and which contains one or more works covered by this license.
6. You may make distributions containing covered files and provide copies of such distributions to whomever you choose, with or without charge, as long as you obey the other terms of this license. Except as stated in (9), you may include as many or as few covered files as you choose in such distributions.
7. When making copies of covered works to distribute to others, you must not remove or alter the Bootstrap License. You may not place your own copyright message, license, or similar statements in the file prior to the

original copyright message or anywhere within the Bootstrap License. Object files and executable files are exempt from the restrictions specified in this clause.
8. If the version of a covered source file as you received it, when compiled, would normally produce executable code that would print a copyright message followed by a message referring to an ISC web page or other ISC documentation, you may not modify the the file in such a way that, when compiled, it no longer produces executable code to print such a message.
9. Any source file covered by this license will specify within the Bootstrap License the name of the ISC distribution from which it came, as well as a list of associated documentation files. The associated documentation for a binary file is the same as the associated documentation for the source file or files from which it was derived. Associated documentation files contain human-readable documentation which the ISC intends to accompany any distribution.

If you produce a distribution, then for every covered file in that distribution, you must include all of the associated documentation files for that file. You need only include one copy of each such documentation file in such distributions.

Absence of required documentation files from a distribution you receive or absence of the list of documentation files from a source file covered by this license does not excuse you from this from this requirement. If the distribution you receive does not contain these files, you must obtain them from the ISC and include them in any redistribution of any work covered by this license. For information on how to obtain required documentation not included with your distribution, see: http://www.isc.org/getting-documentation.html.

If the list of documentation files was removed from your copy of a covered work, you must obtain such a list from the ISC. The web page at http://www.isc.org/getting-documentation.html contains pointers to lists of files for each ISC distribution covered by this license.

It is permissible in a source or binary distribution containing covered works to include reformatted versions of the documentation files. It is also permissible to add to or modify the documentation files, as long as the formatting is similar in legibility, readability, font, and font size to other documentation in the derived product, as long as any sections labeled CONTRIBUTIONS in these files are unchanged except with respect to formatting, as long as the order in which the CONTRIBUTIONS section appears in these files is not changed, and as long as the manual page which describes how to contribute to the Internet Software Consortium (hereafter referred to as the Contributions Manual Page) is unchanged except with respect to formatting.

Documentation that has been translated into another natural language may be included in place of or in addition to the required documentation, so long as the CONTRIBUTIONS section and the Contributions Manual Page are either left in their original language or translated into the new language with such care and diligence as is required to preserve the original meaning.

10. You must include this license with any distribution that you make, in such a way that it is clearly associated with such covered works as are present in that distribution. In any electronic distribution, the license must be in a file called "ISC-LICENSE".

If you make a distribution that contains works from more than one ISC distribution, you may either include a copy of the ISC-LICENSE file that accompanied each such ISC distribution in such a way that works covered by each license are all clearly grouped with that license, or you may include the single copy of the ISC-LICENSE that has the highest version number of all the ISC-LICENSE files included with such distributions, in which case all covered works will be covered by that single license file. The version number of a license appears at the top of the file containing the text of that license, or if in printed form, at the top of the first page of that license.

11. If the list of associated documentation is in a seperated file, you must include that file with any distribution you make, in such a way that the relationship between that file and the files that refer to it is clear. It is not permissible to merge such files in the event that you make a distribution including files from more than one ISC distribution, unless all the Bootstrap Licenses refer to files for their lists of associated documentation, and those references all list the same filename.

12. If a distribution that includes covered works includes a mechanism for automatically installing covered works, following that installation process must not cause the person following that process to violate this license, knowingly or unknowingly. In the event that the producer of a distribution containing covered files accidentally or wilfully violates this clause, persons other than the producer of such a distribution shall not be held liable for such violations, but are not otherwise excused from any requirement of this license.

13. COVERED WORKS ARE PROVIDED "AS IS". ISC DISCLAIMS ALL WARRANTIES WITH REGARD TO COVERED WORKS INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

14. IN NO EVENT SHALL ISC BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OF COVERED WORKS.

Use of covered works under different terms is prohibited unless you have first obtained a license from ISC granting use pursuant to different terms. Such terms may be negotiated by contacting ISC as follows:

Internet Software Consortium
950 Charter Street
Redwood City, CA 94063
Tel: 1-888-868-1001 (toll free in U.S.)
Tel: 1-650-779-7091
Fax: 1-650-779-7055
Email: info@isc.org
Email: licensing@isc.org

DNSSAFE LICENSE TERMS
This BIND software includes the DNSsafe software from RSA Data Security, Inc., which is copyrighted software that can only be distributed under the terms of this license agreement.

The DNSsafe software cannot be used or distributed separately from the BIND software. You only have the right to use it or distribute it as a bundled, integrated product.

The DNSsafe software can ONLY be used to provide authentication for resource records in the Domain Name System, as specified in RFC 2065 and successors. You cannot modify the BIND software to use the DNSsafe software for other purposes, or to make its cryptographic functions available to end-users for other uses.

If you modify the DNSsafe software itself, you cannot modify its documented API, and you must grant RSA Data Security the right to use, modify, and distribute your modifications, including the right to use any patents or other intellectual property that your modifications depend upon.

You must not remove, alter, or destroy any of RSA's copyright notices or license information. When distributing the software to the Federal Government, it must be licensed to them as "commercial computer software" protected under 48 CFR 12.212 of the FAR, or 48 CFR 227.7202.1 of the DFARS.

You must not violate United States export control laws by distributing the DNSsafe software or information about it, when such distribution is prohibited by law.

THE DNSSAFE SOFTWARE IS PROVIDED "AS IS" WITHOUT ANY WARRANTY WHATSOEVER. RSA HAS NO OBLIGATION TO SUPPORT, CORRECT, UPDATE OR MAINTAIN THE RSA SOFTWARE. RSA DISCLAIMS ALL WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO ANY MATTER WHATSOEVER, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS.
If you desire to use DNSsafe in ways that these terms do not permit, please contact:

Contents

Preface

Chapter 1 Installing and Upgrading MultiNet for OpenVMS

Preface

Installation Material

Process Software's MultiNet for OpenVMS consists of software compatible with the TCP/IP (Transmission Control Protocol/Internet Protocol) and the associated networking utilities and programming libraries. MultiNet works on systems running VAX/VMS V5.0 or later, OpenVMS VAX V6.0 or later, and OpenVMS Alpha V1.5 or later.

The V4.3 Consolidated Distribution contains all files required for installing or upgrading to MultiNet Version 4.3. When you install MultiNet, the following components are automatically installed also:

- IP transport
- TCP/IP applications
- MultiNet NFS Client
- MultiNet NFS Server
- TCP/IP Services for DECnet Applications
- MultiNet Secure/IP

Chapter 1 describes how to install and upgrade any combination of these components. The chapter also describes how to establish basic IP connectivity over a standard network interface, and where to find additional configuration documentation for each component.

To install MultiNet in a VMScluster environment, follow the procedures in Chapter 1 for each node. You can skip several steps after you have installed MultiNet on one VMScluster node of a given architecture (VAX or Alpha). In particular, when installing MultiNet for the first time, you need only configure each node; when upgrading, it may be sufficient merely to reboot.

Chapter 2 contains examples of various installation tasks.

Chapter 3 lists the files that may be added to or modified on your system disk during the installation.

Chapter 4 describes how to remove MultiNet from your OpenVMS system.

Introductory Material

In **Chapters 5 through 8**, you will find:

- A description of the MultiNet documentation set
- An introduction to MultiNet and TCP/IP networking concepts
- A list of devices and protocols supported by MultiNet and a brief look at MultiNet internals
- Suggestions for further reading, including where to find Requests for Comments (RFCs) that define networking protocols

MultiNet Documentation

The MultiNet documentation set consists of the following guides:

Title	**Description**
MultiNet for OpenVMS Consolidated Release Notes	Describes new features in the software, descriptions of known restrictions or problems, and corrections to the published MultiNet for OpenVMS documentation. Review the file SYS$HELP:MULTINET043.RELEASE_NOTES after installing the software.
MultiNet for OpenVMS Installation and Introduction	Explains how to install MultiNet and the layered products, and provides an introduction to the MultiNet software. This guide is a compilation of two guides released with older versions of MultiNet: the *MultiNet Installation Guide* and the *Introduction to MultiNet*.
MultiNet for OpenVMS User's Guide	Explains how to explore your network, send and receive electronic mail, log into a remote system, transfer files between systems, use the World Wide Web browser, and use DECwindows with MultiNet; includes user command references.
MultiNet for OpenVMS Administrator's Guide	Explains how to configure and manage MultiNet.
MultiNet for OpenVMS Administrator's Reference	Identifies and describes the MultiNet configuration and management commands
MultiNet for OpenVMS Messages and Logicals Reference	Lists MultiNet messages and provides troubleshooting information in the message descriptions. Table 3-1 lists the MultiNet logicals.
MultiNet for OpenVMS Programmer's Reference	Describes the MultiNet programming interfaces.

Title	Description
TCP/IP Services for DECnet Applications	Explains how to configure TCP/IP Services for DECnet Applications.

To view the current release notes, look on the CD-ROM. The release notes are in TXT format and can be printed.

Typographical Conventions

Examples in this guide use the following conventions:

Convention	Example	Meaning
Bold text	**YES**	Represents user input in instructions or examples.
Bold, uppercase Courier text	**RETURN**	Represents a key on your keyboard.
Bold Courier text with a slash	**Ctrl/A**	Indicates that you hold down the key labeled **CONTROL** or **Ctrl** while simultaneously pressing another key; in this example, the "A" key.
A vertical bar within braces	{ ON | OFF }	Indicates a list of values permitted in commands. The vertical bar separates alternatives; do not type the vertical bar in the actual command.
Italicized text	*file_name*	Represents a variable placeholder; introduces new terminology or concepts; emphasizes something important; represents the title of a book or publication.
Square brackets	[FULL]	Indicates optional choices; you can enter none of the choices, or as many as you like. When shown as part of an example, square brackets are actual characters you should type.
Underscore or hyphen	*file_name* or *file-name*	Between words in commands, indicates the item is a single element.

Obtaining Customer Support

Process Software provides customer support if you have a current Maintenance Service Agreement. If you obtained MultiNet from an authorized distributor or partner, you receive your customer support directly from them.

You can contact Customer Support by:

- Sending electronic mail (see the section Sending Electronic Mail).
- Calling the Customer Support Specialist (see the section Calling Customer Support).
- Fax a description of your problem to the Customer Support Group (see the section Contacting

Customer Support by Fax).

Before Contacting Customer Support

Before you call, or send e-mail or a fax, please:

1. Verify that your Maintenance Service Agreement is current.
2. Read the Release Notes.
3. Have the following information available:
   - Your name
   - Your company name
   - Your e-mail address
   - Your voice and fax telephone numbers
   - Your Maintenance Agreement Number
   - OpenVMS architecture
   - OpenVMS version
   - MultiNet layered products and versions
4. Have complete information about your configuration, error messages that appeared, and problem specifics.
5. Be prepared to let an engineer connect to your system either with TELNET or by dialing in using a modem. Be prepared to give the engineer access to a privileged account to diagnose your problem.

You can obtain information about your OpenVMS architecture, OpenVMS version, MultiNet version, and layered products with the MULTINET SHOW /LICENSE command. For example:

```
$ MULTINET SHOW /LICENSE

Process Software MultiNet V4.3, VAXstation 4000-90, OpenVMS VAX V7.1
```

In this example:

- The machine or system architecture is VAX.
- The OpenVMS version is V7.1.
- The MultiNet version is V4.3.

You can use the following table as a template to record the relevant information about your system

System Information

Required Information	Your System Information
Your name	
Company name	
Your e-mail address	
Your voice and fax telephone numbers	
System architecture	VAX | Alpha
OpenVMS version	
MultiNet version	
MultiNet optional software components:	
- MultiNet NFS Client	Installed? Yes | No
- MultiNet NFS Server	Installed? Yes | No
- MultiNet Secure/IP Client	Installed? Yes | No
- MultiNet Secure/IP Server	Installed? Yes | No
- TCP/IP applications	Installed? Yes | No
- Online documentation	Installed? Yes | No
- MultiNet Programmer's Kit	Installed? Yes | No

Sending Electronic Mail

For many questions, electronic mail is the preferred communication method. Customer support via electronic mail is available to customers with a current support contract. Send electronic mail to **support@process.com**

At the beginning of your mail message, include the information listed in the section *Before Contacting Customer Support*. Continue with the description of your situation and problem specifics. Include all relevant information to help your Customer Support Specialist process and track your electronic support request.

Electronic mail is answered Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

Calling Customer Support

For regular support issues, call 800-394-8700 or 508-628-5074 for support Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

For our customers in North America with critical problems, an option for support 7 days per week,

24 hours per day is available at an additional charge. Please contact your account representative for further details.

Before calling, have available the information described in *Before Contacting Customer Support*. When you call, you will be connected to a Customer Support Specialist.

Be prepared to discuss problem specifics with your Customer Support Specialist and to let that person connect to your system.

If a Specialist is not immediately available, your call will be returned as soon as possible.
Contacting Customer Support by Fax

You can send fax transmissions directly to Customer Support at 508-879-0042.

Before faxing comments or questions, complete the steps in *Before Contacting Customer Support* and include all your system information at the beginning of your fax message. Continue with the description of your situation and problem specifics. Include all relevant information to help your Customer Support Specialist process and track your fax support request.

Faxed questions are answered Monday through Thursday from 8:30 a.m. to 7:00 p.m., and on Friday from 8:30 a.m. to 5:00 p.m. United States Eastern Time.

Obtaining Online Help

Extensive information about MultiNet is provided in the MultiNet help library. For more information, use the following command:

```
$ HELP MULTINET
```

MultiNet Frequently Asked Questions List

You can obtain an updated list of frequently asked questions (FAQs) and answers about MultiNet products from the Process Software home page located at **http://www.process.com**

Accessing the MultiNet Public Mailing List

Process Software maintains two public mailing lists for MultiNet customers:

- **Info-MultiNet@process.com**
- **MultiNet-Announce@process.com**

The **Info-MultiNet@process.com** mailing list is a forum for discussion among MultiNet system managers and programmers. Questions and problems regarding MultiNet can be posted for a response by any of the subscribers. To subscribe to Info-MultiNet, send a mail message with the word “SUBSCRIBE” in the body to Info-MultiNet-request@process.com. The information exchanged over Info-MultiNet is also available via the USENET newsgroup vmsnet.networks.tcp-ip.multinet.

You can retrieve the Info-MultiNet archives by anonymous FTP to ftp.multinet.process.com. The archives are located in the directory [CUSTOMER_SUPPORT.MAIL_ARCHIVES.INFO-MULTINET].

You can also find the Info-MultiNet archives on the MultiNet consolidated CD-ROM in the [CONTRIBUTED-SOFTWARE.LIST-ARCHIVES.INFO-MULTINET] directory.

The **MultiNet-Announce@process.com** mailing list is a one-way communication (from Process Software to you) used for the posting of announcements relating to MultiNet (patch releases, product releases, etc.). To subscribe to MultiNet-Announce, send a mail message with the word "SUBSCRIBE" in the body to MultiNet-Announce-request@process.com.

Process Software World Wide Web Server

Electronic support is provided through the Process Software World Wide Web server, which you can access with any World Wide Web browser; the URL is **http://www.process.com** (select **Customer Support**).

Obtaining Software Patches Over the Internet

Process Software provides software patches in save set and ZIP format on its anonymous FTP server, ftp.multinet.process.com. For the location of software patches, read the .WELCOME file in the top-level anonymous directory. This file refers you to the directories containing software patches.

To retrieve a software patch, enter the following commands:

```
$ MULTINET FTP /USERNAME=ANONYMOUS/PASSWORD="emailaddress"
FTP.MULTINET.PROCESS.COM
```

A message welcoming you to the Process Software FTP directory appears next followed by the FTP prompt. Enter the following at the prompts:

```
FTP.MULTINET.PROCESS.COM>CD [CUSTOMER_SUPPORT.SOFTWARE_UPDATES_VMS.Vnn]

FTP.MULTINET.PROCESS.COM>GET update_filename
```

- *emailaddress* is your e-mail address in the standard *user@host* format.
- *nn* is the version of MultiNet you want to transfer.
- *update_filename* is the name of the file you want to transfer.

To transfer files from Process Software directly to an OpenVMS system, you can use the GET command without any other FTP commands. However, if you need to transfer a software patch through an intermediate non-OpenVMS system, use BINARY mode to transfer the files to and from that system.

In addition, if you are fetching the software patch in save set format, make sure the save set record size is 2048 bytes when you transfer the file from the intermediate system to your OpenVMS system:

- If you use the GET command to download the file from the intermediate system, use the **FTP RECORD-SIZE 2048** command *before* transferring the file.
- If you use the PUT command to upload the file to your OpenVMS system, log into the intermediate system and use the FTP **quote site rms recsize 2048** command before transferring

the file.

Process Software also supplies UNZIP utilities for OpenVMS VAX and Alpha for decompressing ZIP archives in the [THIRD_PARTY_TOOLS.VMS] directory. To use ZIP format kits, you need a copy of the UNZIP utility.

The following example shows how to use the UNZIP utility, assuming you have copied the appropriate version of UNZIP.EXE to your current default directory.

```
$ UNZIP := $SYS$DISK:[]UNZIP.EXE

$ UNZIP filename.ZIP
```

Use VMSINSTAL to upgrade your MultiNet system with the software patch.

Documentation Comments

Your comments about the information in this guide can help us improve the documentation. If you have corrections or suggestions for improvement, please let us know.

Be as specific as possible about your comments: include the exact title of the document, version, date, and page references as appropriate.

You can send your comments by e-mail to: techpubs@process.com or mail the completed form to:

Process Software
959 Concord Street
Framingham, MA 01701-4682
Attention: Marketing Manager

You can also fax the form to us at 508-879-0042.

Your comments about our documentation are very much appreciated.

Chapter 1

Installing and Upgrading MultiNet for OpenVMS

Table 1-1 lists the steps required to install MultiNet. As indicated by the footnotes, you need only perform some of the steps if you are installing this version of MultiNet for the *first time*; you can skip some steps if you have already installed this version of MultiNet on one VMScluster node of the same architecture (VAX or Alpha). The sections in this chapter provide detailed information about each step.

Table 1-1 Installation Steps

Step	Read the Section...
1	*Gather Information for the Installation*
2	*Before Installing MultiNet Secure/IP*
3	*Read the Release Notes*
4	*Check OpenVMS and Versions*
5	*Use the Correct Media*
6	*Back Up Your System Disk*
7	*Reserve Sufficient Disk Space*
8	*Log on as SYSTEM*
9	*Ask Other Users to Log Off*
10	*Update System Parameters*
11	*Check the Location of the DCLTABLES.EXE File*
12	*Review the MultiNet Directory Layout*
13	*Load the PAK (Product Authorization Key)*
14	*Run VMSINSTAL*

Table 1-1 Installation Steps (Continued)

Step	Read the Section...
15	*Establish an Initial Configuration*
16	*Configure the IP Transport Over the Standard Network Interface*
17	*After Installing MultiNet Secure/IP*
18	*Start the New Version of MultiNet*
19	*Modify the System Startup Command Procedure*
20	*Configure Services*
21	*Add or Update User Exits*
22	*Install MultiNet Commands in the DCLTABLES.EXE File*
23	*Set up the Online Documentation*

Configuration procedures allow you to configure IP connectivity using one Compaq LAN interface.

However, you can upgrade MultiNet without changing your existing configuration. As a result, if you upgrade MultiNet on one node in a VMScluster environment, you only need to reboot other nodes of the same architecture to have the upgrade take effect.

Gather Information for the Installation

During installation, you have the option of configuring IP connectivity for the first network device the configuration procedure finds. If you plan to perform this initial configuration, gather the required information before running VMSINSTALL. Table 1-2 lists the information you must gather. (The table also provides a convenient place for you to record this information so you may refer to it later during the installation.)

If the default configuration is not appropriate for your system, you can configure MultiNet after completing the installation, as described in the *Administrator's Guide*.

Note! If you are upgrading a system already running MultiNet, you do not have to configure anything unless you want to change the existing configuration.

Table 1-2 IP Transport Parameter Checklist

Parameter Name	Description	Your Value
Internet host name	The name by which your system will be known. If you plan to use DNS to resolve host names, you must use the fully qualified host name supplied by your network administrator or Internet access provider (for example, BIGBOOTE.FLOWERS.COM). Note: It is generally a good idea to use the well-known name for this host; other systems will rely on DNS or host tables to resolve your host name to the appropriate IP address.	
IP address	The dotted-decimal representation of your system's IP address. For example, the address 191.87.34.22 is a class B IP address in which 191.87 is the network number and 34.22 is the host number. Obtain your IP address from your network administrator or Internet access provider.	
Subnet mask	The dotted-decimal representation of a 32-bit mask that determines the network portion of your IP address to allow your network to be subdivided into multiple network segments. For example: If your IP address is 191.87.34.22, and your subnet mask is 255.255.255.0, your network number is 191.87.34 instead of 191.87 (the network number implied by the class B IP address), and your host number is 22 instead of 34.22. Obtain your subnet mask from your network administrator or Internet access provider.	
Default route	The dotted-decimal representation of the IP address of the router to which IP packets are sent when there is no route to the destination host or network in your system's routing table. The default route must have the same network number as your system. For example: If your IP address is 191.87.34.22, and your subnet mask is 255.255.255.0, 191.87.34.15 can be a valid default route, but 191.87.57.15 (on a different subnet) cannot be. Obtain the default route from your network administrator or Internet access provider.	

Table 1-2 IP Transport Parameter Checklist (Continued)

Parameter Name	Description	Your Value
Use DNS	The answer to the question, "Does your system have access to the Internet to take advantage of DNS (Domain Name System) to resolve host names to IP addresses?". Ask your network administrator or Internet access provider. If your system does not have access to the Internet, you will not be able to resolve host names after completing the installation until you configure the DNS server or host tables on your system (see the *Administrator's Guide*).	Yes | No
Timezone	The standard abbreviation for your local timezone (For example: EST, CST, MST, or PST). Enter your local timezone, or, if your system clock is not in the local timezone, enter the timezone your system clock uses. When prompted for your timezone, type a question mark (?) to see a list of valid timezone abbreviations. Switching between Standard Time and Daylight Savings Time occurs automatically.	

Before Installing MultiNet Secure/IP

Perform the following tasks before installing MultiNet Secure/IP:

- Decide which nodes will act as MultiNet Secure/IP authentication *servers* and which will be authentication *clients*. Install the MultiNet Secure/IP Client on every OpenVMS system you want to protect with MultiNet Secure/IP authentication. Your MultiNet Secure/IP license only affects your ability to run MultiNet Secure/IP Server on a single system. You can install MultiNet Secure/IP Client on as many hosts as you like.

Note! The MultiNet Secure/IP Server must have correct name and address mappings (via DNS or host tables) for all MultiNet Secure/IP Clients.

Note! Secure/IP can now be installed as a part of the MultiNet installation if you have one of the following licenses:

- MULTINET
- SECURE_IP
- EDULIB
- EVALUATION

Note! You can install MultiNet Secure/IP on a VMScluster, and configure each node individually to enable the MultiNet Secure/IP Client or the MultiNet Secure/IP Server on selected nodes.

A Kerberos server (KDC) can also be a logical choice for installing the MultiNet Secure/IP Server.

The connection between MultiNet Secure/IP Clients and Servers must be trusted. If physically secure connections are not possible, you can use a Kerberized connection between the MultiNet Secure/IP Clients and Servers. To configure the MultiNet Secure/IP Client and Server to authenticate each other with Kerberos, use the ACCESS-CONFIG SET MUTUAL-AUTHENTICATION command (see Chapter 8 of the *Administrator's Reference Guide*). By default, mutual authentication is disabled. MultiNet Secure/IP Client systems must have valid Kerberos configurations and KERBEROS.SRVTAB files.

Read the Release Notes

The *Release Notes* contain important information about this release that may not be published in this guide or in the other publications in the MultiNet documentation set. You can display or print the *Release Notes* during the installation.

After the installation, you can find the Release Notes in the file SYS$HELP:MULTINET043.RELEASE_NOTES.

The same information is also available on CD-ROM distributions: ([MULTINET043]MULTINET_RELEASE_NOTES.TXT).

Check OpenVMS and Versions

Ensure your system is running VAX/VMS V5.0 or later, OpenVMS VAX V6.0 or later, or OpenVMS Alpha V1.5 or later. If you are not running one of these operating system versions, you *must* upgrade before installing MultiNet.

If you are upgrading from an earlier release of MultiNet, ensure the existing version of MultiNet is V3.1 or later; you cannot upgrade MultiNet directly from V3.0 or earlier versions.

To check your current MultiNet version:

```
$ TYPE MULTINET:MULTINET_VERSION.
```

If you are running a version of MultiNet earlier than V3.1, refer to your old *MultiNet Installation Guide* for instructions on removing MultiNet from your system. Then, install this release of MultiNet as a new installation, *not an upgrade*.

Use the Correct Media

Ensure you have the proper distribution medium: MultiNet is distributed on CD-ROM, TK50 cartridge tape, and 9-track magnetic tape.

All distribution media (except 9-track tape) contains save sets for the VAX/VMS, OpenVMS VAX, and OpenVMS Alpha operating systems.

Note! If you have already installed on another VMScluster node of the same architecture, you do not need to install from the distribution medium again.

Back up Your System Disk

Make a backup copy of your system disk using the OpenVMS BACKUP (or standalone BACKUP)

utility.

Reserve Sufficient Disk Space

If you are installing MultiNet for the first time, ensure you have sufficient disk space.

To find out how much free space is available on your system disk, use the following DCL command:

```
$ SHOW DEVICE SYS$SYSDEVICE
```

The information displayed includes the number of free blocks on the disk. Table 1-3 shows the approximate disk space required for the VAX and Alpha versions of MultiNet.

Table 1-3 Approximate Required Disk Space

Package	VAX	Alpha
MultiNet Base	20000	30000
MultiNet TCP/IP Applications	21000	32000
Documentation	12500	13500
Include and Library Files	3000	4500
MultiNet Secure/IP Files	2000	2400
NFS Client	2000	2800
NFS Server	3000	2800
Total[a]:	64500	90000
Total with temporary free space[b]:	69000	96000
Total if not installing TCP/IP applications[c]:	43500	58000
Extra free space required if not installing TCP/IP applications[c]:	20000	30000

a. Total required if you install everything in the distribution kit.

b. During normal installation, an additional 4,000 blocks of *temporary* free space are required for OpenVMS VAX, and an additional 11,000 blocks of free space are required for OpenVMS Alpha.

c. If you do not install the TCP/IP applications, 20,000 additional blocks of *temporary* free space are required for a VAX installation, and 28,000 additional blocks are required for an Alpha installation. OpenVMS requires these extra blocks to restore the applications save set before removing the TCP/IP applications. **Note:** This extra space is required *only* during the installation process.

Log on as SYSTEM

The installation procedure copies files onto the system disk (or another disk you specify). You must be logged in as user name SYSTEM (or as another fully privileged user) to perform the installation.

Ask Other Users to Log Off

Make sure other users log off the system before you start the installation or before you modify any

system parameters. You may need to reboot.

Update System Parameters

Before installing MultiNet, you may need to update various system parameters.

Note! With the exception of upgrades to Secure/IP, if an earlier release of MultiNet is installed on your system, you do not need to adjust any system parameters.[1]

1 If you are installing MultiNet on your system for the first time, modify SYS$SYSTEM:MODPARAMS.DAT as follows:

- On OpenVMS VAX and VAX/VMS systems, add the following lines to SYS$SYSTEM:MODPARAMS.DAT:

```
MIN_INTSTKPAGES = 10
MIN_CHALLELCNT  = 200
ADD_SPTREQ      = 1700
ADD_GBLSECTIONS = 20
ADD_GBLPAGES    = 340
```

- On OpenVMS Alpha systems, add the following lines to SYS$SYSTEM:MODPARAMS.DAT:

```
MIN_CHANNELCNT  = 200
ADD_GBLSECTIONS = 20
ADD_GBLPAGES    = 1550
```

2 Execute SYS$UPDATE:AUTOGEN.COM to generate a new system parameter file, and reboot your system to activate the new values. Refer to your OpenVMS system management documentation for information about AUTOGEN.

3 If you are going to upgrade MultiNet Secure/IP during the installation, disable LOGINOUT callouts with the following commands:

```
$ MCR SYSMAN
SYSMAN>SET ENVIRONMENT /CLUSTER
SYSMAN>SET PROFILE /PRIVILEGE-CMKRNL
SYSMAN>PARAMETER USE ACTIVE
SYSMAN>PARAMETER SET LGI_CALLOUTS 0
SYSMAN>PARAMETER WRITE ACTIVE
SYSMAN>EXIT
```

1. If you are using host tables instead of DNS, to ensure they load properly, check the size of the NETWORK_DATABASE. and HOSTTBLUK.DAT files, and increase the ADD_GBLPAGES statement value by 1 for each disk block used by these files, and increase the ADD_GBLSECTIONS value by 2, one for each file.

Check the Location of the DCLTABLES.EXE File

Before installing MultiNet, ensure the DCLTABLES.EXE file to which you want the MULTINET verb added resides in the SYS$COMMON:[SYSLIB] directory. VMSINSTAL requires you to do this because it will not update copies of DCLTABLES.EXE in a system-specific directory.

Review the MultiNet Directory Layout

Unless you specify otherwise, the MultiNet installation procedure creates a top-level [MULTINET] directory on your system disk to hold all the MultiNet files. Depending on the platform on which you are installing, a [.AXP_COMMON] or [.VAX_COMMON] subdirectory is created in the [MULTINET] directory. As MultiNet is installed on each node, a node- or system-specific directory is also created in the [MULTINET] directory. System-specific MultiNet files are stored in the node-specific directories, and architecture-common files are stored in either the [.AXP_COMMON] or [.VAX_COMMON] subdirectory.

Note! If you are upgrading from MultiNet V4.0 or earlier, you can choose to upgrade in the old location, or install in a new location.

If you are upgrading an existing directory structure, that structure is retained.

While both [MULTINET.AXP_COMMON] and [MULTINET.VAX_COMMON] can exist in a multi-architecture cluster in the same directory structure, common configuration files will only be shared by similar architecture nodes.

Unless you specify otherwise, the system-specific directory name is determined by the first of the following values that exist:

- The SYSGEN parameter SCSNODE
- The logical name SYS$NODE
- The logical name SYS$TOPSYS

The system-specific directory is created in the [MULTINET] top-level directory.

Two directories are created under each system-specific directory (as shown in Figure 1-1):

MULTINET.DIR	Contains node-specific files.
SYSCOMMON.DIR	A file entry that points to the architecture-specific common directory. (Subsequent node-specific directories are created similarly.)

MultiNet relies on the logical name MULTINET_COMMON_ROOT to locate shared files, and on the logical name MULTINET_ROOT to locate system-specific files. MULTINET_ROOT is a search list of the system-specific directory and the MULTINET_COMMON_ROOT directory. The MultiNet startup command procedure, START_MULTINET.COM, automatically defines these logical names.

Figure 1-1 The MultiNet Directory Structure

```
[MULTINET]
  [.AXP_COMMON]      <--+
       [.MULTINET]      |
  [.SEUSS]              |
       [.MULTINET]      |
       [.SYSCOMMON] ----+ This is a pointer to [MULTINET.AXP_COMMON]
  [.TOMMY]              |
       [.MULTINET]      |
         [.SYSCOMMON] --+ This is also a pointer to [MULTINET.AXP_COMMON]

[.VAX_COMMON]      <--+
     [.MULTINET]      |
[.ZANE]               |
     [.MULTINET]      |
      [.SYSCOMMON] ---+ This is a pointer to [MULTINET.VAX_COMMON]
```

Load the PAK (Product Authorization Key)

In MultiNet version 4.0 and earlier, you needed a Product Authorization Key (PAK) for individual components. Starting with Version 4.1, there is only one PAK. You must register and load the PAK if:

- This is the first time you have installed on your system.
- The VERSION field in your existing PAK is *not* blank.

For more information about PAKs, refer to the Compaq Computer *VMS License Management Utility Manual*. See the section *Load the PAK* for an example of registering and loading a PAK.

In some situations you need to delete existing PAKs. You need to delete the PAKs if:

- You are running a version of VAX/VMS earlier than V5.5.
- You are upgrading from a MultiNet Version 3.5 or earlier to V4.3.
- Need to register a new PAK.

You do not need to delete the PAK if you are upgrading from Version 4.1 to Version 4.3.

To delete any existing PAKs:

```
$ @MULTINET:PAK-DELETE
```

Note! Delete only PAKs for versions issued by TGV or Cisco, or for Version 3.5 issued by Process Software.

To register your new PAK:

1	Start the VMSLICENSE utility with the command: `$ @SYS$UPDATE:VMSLICENSE`
2	Delete any existing PAKs, if you need to do so. See the section *Load the PAK* for guidelines about deleting PAKs. If you are upgrading from a previous version of MultiNet, be sure to complete the upgrade before you reboot your system. ***Note!*** The LMF AMEND option does not work properly and should not be used to alter the state of the MultiNet PAK.
3	Register your new PAK. Answer **YES** when prompted whether you want it loaded.
4	Exit the VMSLICENSE utility when you have registered your new PAK.

Run VMSINSTAL

Before beginning the installation, gather the information described in the section *Gather Information for the Installation.*

When you install the MultiNet Consolidated Distribution, you have the option of installing all included components.

If you are adding a software component, such as MultiNet Secure/IP, to a system already running MultiNet, you must also re-install any software components that were already installed.

If you are upgrading from a previous version of MultiNet and plan to add a software component already running, such as Secure/IP, then you must also re-install that component.

Note! If you are installing MultiNet on one node in a homogeneous VMScluster environment, and have already installed MultiNet on another node of the same architecture, you do not need to run VMSINSTAL; all required files are already in place.

In this procedure, default values appear in square brackets ([*default*]). To accept the default value, press **`RETURN`**. To abort the installation at any time, press **`Ctrl/Y`**.

1	Load your distribution media.

2	Start the VMSINSTAL utility:
	
	`$ @SYS$UPDATE:VMSINSTAL MULTINET043 -`
	`_$ loc [OPTIONS N,AWD=device:[directory]]`
	
	loc is the device/directory where the installation kit is stored. If you are installing MultiNet from:
	
	• CD-ROM, then mount the CD and specify the full path name of the installation save set directory (such as DKB0:[MULTINET043]).
	• Your login directory, use the logical name SYS$LOGIN:.
	• TK50 tape, specify the tape device name (for example, MUA0:).
	
	Use the OPTIONS N parameters if you want to be prompted to view or print the *Release Notes*.
	
	Use the OPTIONS AWD parameters if there is insufficient space on your system disk to accommodate the temporary files created during installation. See the Compaq Computer *VMS System Manager's Manual* for more details about AWD.
	
	Messages similar to the following will appear. The exact wording depends on your system's operating system and architecture:
	
	`OpenVMS AXP Software Product Installation Procedure V7.0`
	`It is 08-NOV-2000 at 11:10.`
	`Enter a question mark (?) at any time for help.`

3	Ensure your system is in the proper state. If you are not logged in as SYSTEM (or as another fully privileged user), or if any user processes are still running, you are alerted before being asked if you want to continue. ***Note!*** Do not continue the installation until you are logged in using a fully-privileged user name such as SYSTEM, and all other users have logged off. You do not, however, need to disable DECnet to install MultiNet. Any such messages are followed by the prompt: `* Do you want to continue anyway [NO]?` When you are ready, enter **YES**. If you enter **NO**, VMSINSTAL stops and control returns to DCL.

4	Make sure you have a reliable copy of your system disk. The installation copies files onto your system disk. The following prompt appears: `* Are you satisfied with the backup of your system disk [YES]?` If your system disk has not been backed up and you would like to back it up now, enter **NO**. The installation procedure terminates and the DCL prompt appears. After you have made a backup copy of your system disk, restart the installation procedure. If your system disk is already backed-up, press **RETURN** or enter **YES**.
5	Indicate whether the media is ready, if necessary. If you are installing from CD-ROM, the installation begins immediately. If you are installing MultiNet from a 9-track magnetic tape or TK50 cartridge, you are prompted to load the first volume. Load the distribution media into the drive, and enter **YES** when you are ready to continue. The following message appears: `%MOUNT-I-MOUNTED, MLTNET mounted on _`*location*`:` VMSINSTAL then begins the MultiNet installation.
6	Process the *Consolidated Release Notes*, if necessary. If you specified the parameters **OPTIONS N** when you started VMSINSTAL in Step 2, you are asked if you want to print or display the *Release Notes*. Respond as desired. For an example of printing the *Release Notes*, see the section *Read the Release Notes* "Sample Installation Dialog".
7	Read the Terms and Conditions displayed in the MultiNet Restricted Rights notice.

8	Ensure proper specification of the MultiNet directory structure. If you are upgrading a running version of MultiNet, the logical names MULTINET_ROOT and MULTINET_COMMON_ROOT will be displayed for verification. If you are upgrading from a version of MultiNet prior to V4.0, the display will have the following form:
	
	`The logicals MULTINET_ROOT and MULTINET_COMMON_ROOT are already defined, with the following values:`
	
	disk`:[SYS`*n*`.][MULTINET]`
	disk`:[SYS`*n*`.SYSCOMMON.][MULTINET]`
	
	If you are upgrading MultiNet V4.0 or later, the display may be of this form:
	
	`The logicals MULTINET_ROOT and MULTINET_COMMON_ROOT are already defined, with the following values:`
	
	disk`:[MULTINET.`*nodename*`.][MULTINET]`
	disk`:[MULTINET.`*nodename*`.SYSCOMMON][MULTINET]`
	
	You are then asked whether you want to upgrade:
	
	`You may either upgrade the version of MultiNet installed in this location, or install a fresh copy of MultiNet in another location.`
	
	`* Do you want to upgrade your MultiNet installation [YES] ?`
	
	If you reply **NO**, or if this is a new installation, you are prompted for an installation location and a name for the system-specific directory:
	
	`* Where do you want to install MultiNet [SYS$SYSDEVICE:[MULTINET]]:`
	
	`* What do you want to call the system-specific directory [VAX01]:`
	
	CAUTION! If you respond NO in Step 8, and install MultiNet in a new location, your new installation will not contain any of your original MultiNet configuration files.
	
	Several lines of copyright notices appear, then you are prompted for each component installation.

9	Specify the software components you want to install. ***Note!*** If you plan to run MultiNet or MultiNet Secure/IP on any nodes in your VMScluster environment, be sure to install these software components now. Instructions for installing MultiNet Secure/IP begin at the next section. Enter **YES** for each software component you want to install, and **NO** for each one you do not want on your system (previously installed components will be removed). Include all MultiNet products you want to run on any node in your VMScluster environment. ***Note!*** You must install all software components you want to use, even if they are already installed. For example, if you are already running MultiNet TCP/IP applications, and want to install MultiNet Secure/IP, you must install *both* MultiNet Secure/IP *and* the TCP/IP applications.
10	Verify your selections. VMSINSTAL next lists the components to be installed and the software components, if any, to be removed from your system during installation. You are asked if you want to revise the list of software components to be installed or removed: `* Would you like to change your selections [NO]?` To change the list of software components to install, enter **YES**, and repeat Step 9. To accept the list, enter **NO**.

11	Decide whether to install user commands:
	
	`* Do you want to install the user commands in DCLTABLES [YES]?`
	
	This prompt lets you choose whether or not to install additional MultiNet DCL commands in the DCLTABLES.EXE file. Doing this allows you to issue the following commands without the "MULTINET" prefix:
	
	If you are installing MultiNet for *evaluation*, or if you have commands with these same names from another vendor, enter **NO**. You can still access the MultiNet utilities by preceding the command with the keyword MULTINET, or by creating symbols such as:
	
	`% TELNET :== MULTINET TELNET`
	
	Otherwise, enter **YES** to install the user commands in the DCLTABLES.EXE file.
	
	Note! You can install the MultiNet user commands in the DCLTABLES.EXE file after completing the installation.
	
	If you have not installed your MultiNet license PAK, you are warned that you do not have the required license. You can still continue to install MultiNet. To continue the process, enter YES at the following prompt:
	
	`* Do you want to continue the installation anyway [NO]?`
	
	You must register the PAK before you can start and use Multinet. When you finish the installation and configuration, run VMSLICENSE to register the PAK as shown in the section *Load the PAK*.

12	Decide whether to purge files: `* Do you want to purge files replaced by this installation [YES]?` If you want VMSINSTAL to purge files replaced by this version of the software, press **RETURN** or enter **YES**. If you do not want the replaced files to be purged, enter **NO**. ***Note!*** Even if you choose to purge files, the installation procedure does not purge configuration files. ***CAUTION!*** If you upgrade MultiNet in a VMScluster environment, do not purge the old files during installation. Instead, wait until you have rebooted each node in the cluster.

13	Decide whether to configure software components. If you are installing the TCP/IP applications, you are asked if you want to configure those software components after installation. Enter **YES** if you are installing MultiNet for the first time, or if you need to reconfigure.
	
	The installation continues with no additional prompts.
	
	If this is the *first time* you have installed MultiNet, the installation procedure creates the MultiNet directories and copies the files from the distribution kit into those directories.
	
	VMSINSTAL also optionally installs the MultiNet user commands in SYS$LIBRARY:DCLTABLES.EXE. The MULTINET verb is always installed in your DCLTABLES.EXE file.
	
	If you have *previously installed* MultiNet on your system, the installation procedure deletes old copies of files replaced during this installation. A series of %VMSINSTAL-I- and %MULTINET-I- informational messages appear during these operations to indicate which files are being installed, merged, or removed, and the save sets from which they came.
	
	If you chose to configure the TCP/IP applications, respond to the prompts with the information you gathered in the section *Gather Information for the Installation*.
	
	The configuration procedure then compiles the ASCII network, host, and service configuration files into binary format and creates or updates various configuration files. As it performs these operations, it prints a number of informational messages.
	
	Upon completion, the installation procedure print messages similar to the following (the messages may vary with the operating system version running on your system):
	
	`Installation of MULTINET V4.3 completed at 12:15`
	`Adding history entry in VMI$ROOT:[SYSUPD]VMSINSTAL.HISTORY`
	`Creating installation data file:`
	`VMI$ROOT:[SYSUPD]MULTINET043.VMI_DATA`
	`VMSINSTAL procedure done at 12:15`
	`$`
	
	MultiNet is now installed.

Establish an Initial Configuration

When you *upgrade* from an earlier version of MultiNet, all existing configuration settings are preserved *unless* you intentionally change them during installation.

If you are installing MultiNet for the *first time*, however, you have the opportunity during installation to configure the MultiNet IP transport over one standard network interface simply by responding to a series of prompts.

If you have *already installed* MultiNet on one VMScluster node and are now installing MultiNet on another VMScluster node of the same architecture and operating system, or if you chose not to configure MultiNet during the installation, you can configure the MultiNet IP transport over the standard interface using the CONFIGURE.COM command procedure. Gather the required

configuration information before configuring. See the section *Gather Information for the Installation*.

CAUTION! If your system does not have one of the standard network interfaces, do not use CONFIGURE.COM to establish connectivity. If you do not use the command procedure, you will need to manually enter configuration information. For details on establishing connectivity with all supported network interfaces, refer to the *Administrator's Guide*.

Configure the IP Transport Over the Standard Network Interface

Follow these steps to configure the MultiNet IP transport over the standard network interface:

1	Set your default directory to the architecture-specific common directory, *device*:[MULTINET.*arch*_COMMON.MULTINET], *device* is the device you chose in Step 8 of the installation procedure, and *arch* is the architecture (either VAX or AXP).
2	The MultiNet configuration command procedure CONFIGURE.COM provides a default location for the new node-specific directories and prompts you for correction. It will create the new directories and logical names to get your system up and running on the local subnet by prompting you for the information in your configuration checklist (see the section *Gather Information for the Installation*). To run the command procedure, type: `$ @CONFIGURE`

After Installing MultiNet Secure/IP

If this is the first time you are installing MultiNet Secure/IP, follow Table 1-4

Table 1-4 After Installing MultiNet Secure/IP

Task	**See the Section...**
To use the Security Dynamics method	*Using SECURID_CLIENT_CHECK*
To configure your network firewalls	*Configuring Firewalls*
To unpack the S/KEY clients for PC and Mac users	*Unpacking S/KEY Clients for PC and Apple Macintosh Users*

Note! If you are upgrading MultiNet Secure/IP from an earlier release, your configuration is preserved. If you are installing for the first time, you *must* configure MultiNet Secure/IP as described in Chapter 4 of the *Administrator's Guide*.

Using SECURID_CLIENT_CHECK

If you are using the Security Dynamics method:

1	Copy the file */var/ace/sdconf.rec* from the ACE/Server to the MULTINET: directory (MULTINET_COMMON_ROOT:[MULTINET] on a VMScluster).

2	Verify that the Security Dynamics *sdconf.rec* file contains meaningful data with the SECURID_CLIENT_CHECK program, as shown in the following example:
	
	`$ DIR /SECURITY MULTINET:SDCONF.REC`
	`Directory MULTINET_ROOT:[MULTINET] SDCONF.REC;1 [1,4] RWED,RWED,,)`
	`Total of 1 file.`
	
	`$ RUN MULTINET:SECURID_CLIENT_CHECK`
	`read configuration file function configuration file is version 1`
	`The configuration structure is 356 bytes long`
	`The ACE/Server limits are:`
	`Client retry is 5 times and the Client timeout is 3 seconds`
	`There is a master and a slave configured`
	`DES has been enabled with sdconfig`
	`Duress mode has been disabled by sdconfig`
	`Addresses are resolved by name service`
	`Number of bad Cardcodes is 3`
	`Number of bad PINS is 3`
	`master = mel-brooks`
	`The address of the master ACE/Server is 161.44.224.66`
	`slave = hq`
	`The address of the slave ACE/Server is 161.44.224.70`
	`sdpropd_port is 5510`
	`The service name is securid`
	`acmprotocol = udp`
	`acm_port is 2200`

Configuring Firewalls

When a network has a gateway system that controls all incoming access, that gateway is known as a firewall. To allow MultiNet Secure/IP to authenticate users, firewalls must accept incoming TELNET access and silently connect authorized users with RLOGIN to their actual login. The MULTINET_ROOT:[MULTINET.EXAMPLES]CAPTIVE-LOGIN.COM file is an example of a command procedure that provides a captive RLOGIN service for those using TELNET to access a host from over the network. This command procedure can also be used to remind users not to enter their passwords over any unprotected communication channel from which their TELNET session originates.

When you use this command procedure, RLOGIN must be enabled on the local hosts to which users will connect.

To use CAPTIVE-LOGIN.COM:

1	Create accounts on the firewall for all MultiNet Secure/IP users.
2	Use OpenVMS AUTHORIZE to ensure this procedure is invoked when users log in.
3	Copy the command procedure from the EXAMPLES directory to the SYS$MANAGER: directory.

The following example demonstrates these steps:

```
$ SET PROC/PRIV=SYSPRV
$ SET DEF SYS$SYSTEM
$ RUN AUTHORIZE
UAF>ADD FRED/LGICMD=SYS$MANAGER:INTERNET-LOGIN.COM/FLAG=(CAPTIVE) -
_UAF>/DIR=[FRED]/UIC=[123,123]
%UAF-I-ADDMSG, user record successfully added
%UAF-I-RDBADDMSGU, identifier FRED value [000123,000123] added to rights
database
UAF>EXIT
%UAF-I-DONEMSG, system authorization file modified
%UAF-I-NAFNOMODS, no modifications made to network proxy database
%UAF-I-RDBDONEMSG, rights database modified
$ COPY MULTINET_ROOT:[MULTINET.EXAMPLES]CAPTIVE-LOGIN.COM -
_$ SYS$MANAGER:INTERNET-LOGIN.COM
$ SET FILE/OWNER=[1,4]/PROTECTION=(S:RWED,O:RWED,G:RE,W:RE) -
_$ SYS$MANAGER:INTERNET-LOGIN.COM
```

Unpacking S/KEY Clients for PC and Apple Macintosh Users

If you use the S/KEY method, Apple Macintosh and PC client programs are provided in the MULTINET_COMMON_ROOT:[EXAMPLES] directory. The MACOPIE.HQX file in this directory contains the Macintosh client, which can be unpacked with Stuffit. The SKEY-DOS.BCK file contains the PC client, which can be unpacked with the OpenVMS BACKUP utility.

You can also download the Macintosh and PC client programs over the Internet from thumper.bellcore.com by anonymous FTP to the /pub/skey directory. MacOpie is also available from the Info-Mac archives and its associated mirrors.

Note! MacOpie uses the MD5 Message Digest algorithm by default. To use MacOpie with MultiNet Secure/IP, the MD4 Message Digest must be selected under the References menu section.

Start the New Version of MultiNet

If you installed MultiNet on a system *already running* MultiNet, perform these four steps after completing the installation to ensure its success; MultiNet then starts automatically:

1	Recompile the host lookup table:[a] $ **MULTINET HOST_TABLE COMPILE**
2	Reboot your system to load the new kernel.
3	Run the MultiNet CheckOut Utility. $ **MULTINET CHECK**
4	Rectify any problems found.

a. Recompiling the host lookup table is only necessary on the first node of a given architecture in a VMScluster environment.

If you have successfully installed and configured MultiNet for the *first time* on your system, as described in the previous sections, you are ready to start MultiNet. You do not have to reboot if your system has never run any TCP/IP stack; however, you may need to reboot after running AUTOGEN to activate any system parameter changes you made.

Successful configuration of MultiNet defines the logical name MULTINET and creates the file MULTINET:START_MULTINET.COM. However, if you have rebooted, the MULTINET logical may not be defined. Ensure the logical name is defined. Enter:

```
$ SHOW LOGICAL MULTINET
```

Also ensure the file exists. Enter:

```
$ DIRECTORY MULTINET:START_MULTINET.COM
```

If the logical name and the file are not present, check for installation errors and configuration problems, and correct them before proceeding. If they are not present because you rebooted, then add the following line to your system startup command procedure:

```
$ @SYS$SYSDEVICE:[MULTINET.HYDRA.MULTINET]START_MULTINET
```

To locate the startup command procedure, enter the following:

```
$ DIR SYS$SYSDEVICE: [000000...]START_MULTINET.COM
Directory SYS$SYSDEVICE:MULTINET.HYDRA.MULTINET]
START_MULTINET.COM;1
```

Use the following commands to start MultiNet:

```
$ REPLY/ENABLE=NETWORK/TEMPORARY
$ @MULTINET:START_MULTINET
```

You may use the MULTINET logical name here, as it is defined by the configuration procedures. Be sure your system startup command procedure refers to the disk and directory where you installed MultiNet.

Note! Regardless of where you installed MultiNet, you do not have to define the MULTINET logical name—this is done automatically in the first lines of the START_MULTINET.COM command procedure.

Modify the System Startup Command Procedure

If you are *upgrading* from MultiNet V3.*n* to V4.3, but want to retain the old directory structure—or you are upgrading a MultiNet V4.*n* system that is already using the new directory structure introduced with MultiNet V4.0 Rev A—you do not need to make any changes to your system startup command procedure.

If you are *upgrading* from MultiNet V3.*n* to V4.3, and chose to adopt the new directory structure, modify the existing START_MULTINET.COM call in your system startup command procedure. Edit the procedure as follows:

```
$ @device:[directory.nodename.MULTINET]START_MULTINET.COM
```

device, *directory*, and *nodename* correspond to those you chose in Step 8 of the installation procedure.[1]

If you are installing MultiNet for the *first time*, add the following line to your system startup command procedure:

```
$ @device:[directory.nodename.MULTINET]START_MULTINET.COM
```

device, *directory*, and *nodename* correspond to those you chose in Step 8 of the installation procedure.[1]

Note! The START_MULTINET.COM file will not exist until you configure MultiNet

If you are running a version of VAX/VMS prior to V5.5, add the START_MULTINET.COM call to your system startup procedure after the command that starts the OpenVMS queue manager (START/QUEUE/MANAGER). With VAX/VMS V5.5 and later, and with all versions of OpenVMS Alpha, the queue manager starts automatically.

If you are also running DECnet, ensure the call to the MultiNet startup procedure is placed after the call to SYS$MANAGER:STARTNET.COM.

Configure Services

Once you have established IP, you can configure services and other components. Table 1-5 indicates where to locate documentation on configuring standard services and the optional components you can install.

Note! Additional information about these services may be found in the *Release Notes*.

1. If the name of your system is HOBBES, and you chose the default values for your V4.0 directory structure, the startup command will read $ @SYS$SYSDEVICE:[MULTINET.HOBBES.MULTINET]START_MULTINET.COM

Table 1-5 Where to Find Information about Configuring Services

To configure this service...	See this MultiNet publication
GATED (IP Routing)	*Administrator's Guide*
DNS (Domain Name System)	*Administrator's Guide*
DHCP (Dynamic Host Configuration Protocol)	*Administrator's Guide*
NTP (Network Time Protocol)	*Administrator's Guide*
SMTP (Simple Mail Transfer Protocol)	*Administrator's Guide*
LPD (Line Printer Daemon) printing services	*Administrator's Guide*
RMT (Remote Tape) Services	*Administrator's Guide*
FTP (File Transfer Protocol) Server	*Administrator's Guide*
XDM (X Display Manager)	*Administrator's Guide*
Font Server	*Administrator's Guide*
SNMP (Simple Network Management Protocol)	*Administrator's Guide*
Kerberos Authentication	*Administrator's Guide*
NFS (Network File System) Client	*Administrator's Guide*
NFS (Network File System) Server	*Administrator's Guide*
X11 Gateway	*Administrator's Guide*
DECnet-over-IP	*Administrator's Guide*
MultiNet Secure/IP	*Administrator's Guide*
Secure Shell (SSH) Server Secure Shell (SSH) Client	*Administrator's Guide* *User's Guide*
TCP/IP Services for DECnet Applications	*TCP/IP Services for DECnet Applications*

Add and Update User Exits

MultiNet allows you to customize some functions through the use of *user exits.* If you are upgrading MultiNet and have modified any user exits prior to this installation, merge your modifications into the user exits replaced during the installation. For more information about customizing user exits, see the *Administrator's Guide*.

Install MultiNet Commands in the DCLTABLES.EXE File

If you did not install the MultiNet user commands in the DCLTABLES.EXE file during installation, you can install them manually with the following commands:

```
$ SET COMMAND /TABLES=SYS$COMMON:[SYSLIB]DCLTABLES -
_$ /OUTPUT=SYS$COMMON:[SYSLIB]DCLTABLES MULTINET:USER.CLD
$ INTALL REPLACE SYS$COMMON:[SYSLIB]DCLTABLES
```

Before Running Secure Shell (SSH)

You must enter the following code to the SYLOGIN.COM file before you run Secure Shell. This code needs to be added in a section that is executed when doing an interactive login:

```
SSH_SYS = "TCPWARE"
$ IF F$TRNLNM("MULTINET") .NES. "" THEN SSH_SYS = "MULTINET"
```

Galaxy Shared Memory

MultiNet supports IP over Galaxy Shared Memory interfaces. Configuration is the same as any Ethernet or FDDI (se) device.

MULTINET SET/INTERFACE sets the MTU of an interfacce automatically to the maximum byte size revealed by the VMS device, if available. This allows for more devices to get their proper MTU setting automatically, without defaulting to 1500 or having to be set by the system manager with the /MTU qualifier.

Chapter 2

Example Procedures

This chapter contains example procedures that show the prompts you encounter when registering the PAK and during the installation procedure. The user responses, which appear in **bold** typeface, are provided only to illustrate how you may respond. *Do not use these responses for your installation!* Use the configuration information you gathered in Section 1.1.

Installing a License PAK

This section presents an example dialog showing how to use the VMSLICENSE REGISTER option with a PAK (Product Authorization Key).

The values shown in Example 2-1, "Registering and Loading a PAK," are only examples. When you use the VMSLICENSE REGISTER option, use the actual values provided with your PAK.

Note! Refer to Section 1.12, "Load the PAK (Product Authorization Key)," for the procedure to use for registering the PAK on software upgrades.

Refer to the Compaq Computer *VMS License Management Utility Manual* for more information about PAKs.

Example 2-1 Registering and Loading a PAK

```
$ @SYS$UPDATE:VMSLICENSE
VMS License Management Utility Options:
1. REGISTER a Product Authorization Key
2. AMEND an existing Product Authorization Key
3. CANCEL an existing Product Authorization Key
4. LIST the Product Authorization Keys
5. MODIFY an existing Product Authorization Key
6. DISABLE an existing Product Authorization Key
7. DELETE an existing Product Authorization Key
8. COPY an existing Product Authorization Key
9. MOVE an existing Product Authorization Key
10. ENABLE an existing Product Authorization Key
```

```
   11. SHOW the licenses loaded on this node
   12. SHOW the unit requirements for this node

   99. EXIT this procedure

   Type '?' at any prompt for a description of the information requested.
   Press Ctrl/Z at any prompt to exit this procedure.
   Enter one of the above choices [1] 1
   Do you have your Product Authorization Key? [YES] RETURN

   Use the REGISTER option to add a new license to a license database.  A
   Product Authorization Key (PAK) provides the product name and information
   you need to register the license.  You must enter all the information
   provided by your PAK exactly as it appears.

   Issuer [DEC]:PROCESS SOFTWARE
   Authorization Number []:B-400-17904
   Product Name [ ]:  MULTINET
   Producer [DEC]:PROCESS SOFTWARE
   Number of Units []:100
   Version []:
   Product Release Date []:23-MAR-2000
   Key Termination Date []RETURN
   Availability Table Code []F|
   Activity Table Code []RETURN
   Key Options []NO_SHARE

   This Product Authorization Key (PAK) has been provided with the NO_SHARE
   option.  If it is to be used by a node in a cluster, this PAK must be
   restricted to a specific node.

   If this PAK is to be used by a standalone system, answer NO to the
   following question.

   Is this PAK restricted to a cluster member node? [YES]: RETURN

   Note:  For the majority of systems, the SCS node name is the same as the
   DECnet node name.

   Node this PAK is restricted to (SCS Node name) [] MIGUEL
   Product Token [] AB-400-17904
   Hardware-Id [] RETURN
   Checksum [] 4-IPMA-KEIL-PCOP-HNNJ

   Here is a list of the license information just entered:

   Issuer:  PROCESS SOFTWARE
   Authorization:  B-400-17904
   Producer:  PROCESS SOFTWARE
   Units:  100
```

```
Release Date:  23-MAR-2000
Version:
Termination Date:
Availability:  F
Activity:
Options:  NO_SHARE
Token:  AB-400-17904
Hardware ID:
Checksum:  4-IPMA-KEIL-PCOP-HNNJ

This authorization key is restricted to: MIGUEL
Is that correct? [YES] RETURN
Do you want to LOAD this license on this system? [YES] RETURN

VMS License Management Utility Options:
1. REGISTER a Product Authorization Key
2. AMEND an existing Product Authorization Key
3. CANCEL an existing Product Authorization Key
4. LIST the Product Authorization Keys
5. MODIFY an existing Product Authorization Key
6. DISABLE an existing Product Authorization Key
7. DELETE an existing Product Authorization Key
8. COPY an existing Product Authorization Key
9. MOVE an existing Product Authorization Key
10.ENABLE an existing Product Authorization Key
11.SHOW the licenses loaded on this node
12.SHOW the unit requirements for this node

99.EXIT this procedure

Type '?' at any prompt for a description of the information requested.
Press Ctrl/Z at any prompt to exit this procedure.

Enter one of the above choices [1] 99
```

Printing the Consolidated Release Notes

Example 2-2, "How to Print the MultiNet Release Notes," shows how to print the *Release Notes*.

Note! The VMSINSTALL kit has first been copied to the directory DUA0:[SWDIST].

Example 2-2 How to Print the MultiNet Release Notes

```
$ @SYS$UPDATE:VMSINSTAL MULTINET043 DUA0:[SWDIST] OPTIONS N
OpenVMS AXP Software Product Installation Procedure V7.0
It is 08-MAR-2000 at 11:10.
Enter a question mark (?) at any time for help.
* Are you satisfied with the backup of your system disk [YES]? RETURN
The following products will be processed:
```

```
MULTINET V4.3
Beginning installation of MULTINET V4.3 at 11:10
%VMSINSTAL-I-RESTORE, Restoring product save set A ...
Release notes included with this kit are always copied to SYS$HELP.
Additional Release Notes Options:
1. Display release notes
2. Print release notes
3. Both 1 and 2
4. None of the above
* Select option [2]: RETURN
* Queue name [SYS$PRINT]: SYS$PRINT
Job MULTINET043 (queue SYS$PRINT, entry 1023) started on LPA0:
* Do you want to continue the installation [NO] ? RETURN
%VMSINSTAL-I-RELMOVED, The product's release notes have been successfully
moved to SYS$HELP.
VMSINSTAL procedure done at 11:11
```

Sample Installation Dialog

This section contains two examples of MultiNet installation procedures:

- Example 2-3, "Sample New Installation," shows a new installation from CD-ROM. (Some messages may vary with the operating system version.)
- Example 2-4, "Sample Upgrade Installation," shows how to upgrade from an older version of MultiNet to the current release. (Some messages may vary with the operating system version.) You must reboot your system after upgrading the software.

Note! *The values shown in the dialogs are samples and for illustration purposes only!* When you install MultiNet, use the actual values appropriate for your system.

Example 2-3 Sample New Installation

```
$ @SYS$UPDATE:VMSINSTAL MULTINET043 DKB300 OPTIONS N
OpenVMS VAX Software Product Installation Procedure V7.1
It is 23-MAR-2000 at 11:17
Enter a question mark (?) at any time for help.
* Are you satisfied with the backup of your system disk [YES] ? RETURN
The following products will be processed:
MULTINET V4.3
Beginning installation of MULTINET V4.3 at 11:17
%VMSINSTAL-I-RESTORE, Restoring product save set A ...
%VMSINSTAL-I-RELMOVED, Product's release notes have been moved to
SYS$HELP.
* Where do  you want to install MultiNet [SYS$SYSDEVICE:[MULTINET]]:RETURN
* What do you want to call the system-specific directory [HOBBES]: RETURN
MultiNet  (R)
ALL RIGHTS RESERVED USER THE COPYRIGHT LAWS OF THE UNITED STATES
```

```
This licensed material is the valuable property of Process Software. Its
use, duplication, or disclosure is subject to the restrictions set forth
in the License Agreement.

Other use, duplication or disclosure, unless expressly provided for in the
license agreement, is unlawful.

Installing MultiNet V4.3
* Do you want to install the TCP/IP applications [YES]? RETURN
* Do you want to install the NFS Client software [YES]? RETURN
* Do you want to install the NFS Server software [YES]? RETURN
* Do you want to install the MultiNet Secure/IP client software [YES]?
RETURN
* Do you want to install the MultiNet Secure/IP server software [YES]?
RETURN
* Do you want to install the online documentation [YES]? RETURN
* Do you want to install the include and library files [YES]? RETURN

The MultiNet base networking software will be installed with these
selected components:
* TCP/IP applications
* NFS client
* NFS server
* MultiNet Secure/IP Client
* MultiNet Secure/IP Server
* Online documentation
* Include and library files
* Would you like to change your selection [NO]? RETURN
* Do you want to install the user commands in DCLTABLES [YES]? RETURN
* Do you want to purge files replaced by this installation [YES]? RETURN
* Configure MultiNet TCP/IP after installation [NO]? YES
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.SPOOL].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.HELP].
%VMSINSTAL-I-...This product creates...
MU$SPECIFIC_ROOT:[MULTINET.LOADABLE_IMAGES].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.SPOOL].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.HELP].
%VMSINSTAL-I-...This product creates...
MU$COMMON_ROOT:[MULTINET.LOADABLE_IMAGES].
The installation will now proceed with no further questions.
%VMSINSTAL-I-RESTORE, Restoring product save set B...
%VMSINSTAL-I-RESTORE, Restoring product save set C...
%MULTINET-I-INSTALLING, Installing MultiNet base files
%VMSINSTAL-I-RESTORE, Restoring product save set E...
%MULTINET-I-INSTALLING, Installing MultiNet driver files
%VMSINSTAL-I-RESTORE, Restoring product save set G...
%VMSINSTAL-I-RESTORE, Restoring product save set H...
%MULTINET-I-INSTALLING, Installing MultiNet TCP/IP application files
```

```
%VMSINSTAL-I-RESTORE, Restoring product save set J...
%VMSINSTAL-I-RESTORE, Restoring product save set K...
%MULTINET-I-INSTALLING, Installing MultiNet NFS files
%VMSINSTAL-I-RESTORE, Restoring product save set M...
%VMSINSTAL-I-RESTORE, Restoring product save set N...
%MULTINET-I-INSTALLING, Installing MultiNet Secure/IP files
%VMSINSTAL-I-RESTORE, Restoring product save set P...
%MULTINET-I-INSTALLING, Installing the online documentation files
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.DECW$BOOK].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.DECW$BOOK].
%VMSINSTAL-I-RESTORE, Restoring product save set Q...
%VMSINSTAL-I-RESTORE, Restoring product save set R...
%MULTINET-I-INSTALLING, Installing the include and library files
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.ARPA].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.NET].
%VMSINSTAL-I-...This product creates...
MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.NETINET].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.NETNS].
%VMSINSTAL-I-...This product creates...
MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.NETWARE].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.NFS].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.RPC].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.SYS].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.INCLUDE.VMS].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.LIBRARY].
%VMSINSTAL-I-...This product creates...MU$SPECIFIC_ROOT:[MULTINET.EXAMPLES].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.ARPA].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.NET].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.NETINET].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.NETNS].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.NETWARE].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.NFS].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.RPC].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.SYS].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.INCLUDE.VMS].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.LIBRARY].
%VMSINSTAL-I-...This product creates...MU$COMMON_ROOT:[MULTINET.EXAMPLES].

%MULTINET-I-INSTALLING, Installing MultiNet HELP library
%MULTINET-I-DELETING, Deleting obsolete MultiNet files
% VMSINSTAL-I-MOVEFILES, Files will now be moved to their target
directories...
* System Specific directory name: [DKA100:[MULTINET.HOBBES]]: RETURN
* Enter your Internet host name: HOBBES.FLOWERS.COM
* Enter the Internet (IP) Address for interface ESA0: 191.87.34.22
* Enter the Subnet mask for interface ESA0 (optional): 255.255.255.0
Configure other network devices after installation using the $ MULTINET
CONFIGURE utility.
```

```
* Enter the Internet (IP) Address of your default route (optional):
191.87.34.1
* Use Domain Nameservice instead of host tables [YES]? RETURN
* Enter your local timezone: EST
To have MultiNet start automatically when your system boots, add the
following command to your system startup procedure:
$ @DISK$HOBBES:[MULTINET.HOBBES.MULTINET]START_MULTINET.COM
Type a question mark (?) at any prompt for help.
Press Ctrl/Z at any prompt, or Ctrl/Y at any other time, to exit.
* System Specific directory name: [DKB300:[MULTINET.HOBBES]]: RETURN
Enter link-level encapsulation type used on your LAN [RAW-802.3]: ethernet
OK to proceed? YES
MultiNet Network Configuration Utility V4.3 (102)
[Reading in MAXIMUM configuration from MULTINET:MULTINET.EXE]
[Reading in configuration from MULTINET:NETWORK_DEVICES.CONFIGURATION]
[Writing Startup file MULTINET:START_MULTINET.COM]
%MULTINET-I-REBOOT, you must reboot VMS before MultiNet will function
Installation of MULTINET V4.3 completed at 11:46
VMSINSTAL procedure done at 11:47
```

Example 2-4 Sample Upgrade Installation

```
$ @SYS$UPDATE:VMSINSTAL MULTINET043 DKB400 OPTIONS N
OpenVMS AXP Software Product Installation Procedure B7.1
It is 23-MAR-2000 at 12:12.
Enter a question mark (?) at any time for help.
* Are you satisfied with the backup of your system disk [YES]? RETURN
The following products will be processed:
MULTINET V4.3
Beginning installation of MULTINET V4.3 at 12:12
%VMSINSTAL-I-RESTORE, Restoring product save set A ...
%VMSINSTAL-I-RELMOVED, Product's release notes have been moved to
SYS$HELP.
The logical names MULTINET_ROOT and MULTINET_COMMON_ROOT are already
defined, with the following values:
DKA100:[CALVIN.][MULTINET]
DKA100:[CALVIN.SYSCOMMON.][MULTINET]
You may either upgrade the version of MultiNet installed in this location,
or install a fresh copy of MultiNet in another location.
* Do you want to upgrade your MultiNet installation [YES] ? YES
MultiNet (R)
ALL RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES
This licensed material is the valuable property of Process Software. Its
use, duplication, or disclosure is subject to the restrictions set forth
in the License Agreement.
Other use, duplication or disclosure, unless expressly provided for in the
license agreement, is unlawful.
```

```
Installing MultiNet V4.3
* Do you want to install the TCP/IP applications [YES]? RETURN
* Do you want to install the NFS Client software [YES]? RETURN
* Do you want to install the NFS Server software [YES]? RETURN
* Do you want to install the MultiNet Secure/IP client software [YES]?
RETURN
* Do you want to install the MultiNet Secure/IP server software [YES]?
RETURN
* Do you want to install the online documentation [YES]? RETURN
* Do you want to install the include and library files [YES]? RETURN

The MultiNet base networking software will be installed with these
selected components:
* TCP/IP applications
* NFS Client
* NFS Server
* MultiNet Secure/IP Client
* MultiNet Secure/IP Server
* Online documentation
* Include and library files
* Would you like to change your selections [NO]? RETURN
* Do you want to install the user commands in DCLTABLES [YES]? RETURN
* Do you want to purge files replaced by this installation [YES]? RETURN
* Configure MultiNet TCP/IP after installation [NO]? RETURN

The installation will now proceed with no further questions.
%VMSINSTAL-I-RESTORE, Restoring product save set B...
%VMSINSTAL-I-RESTORE, Restoring product save set D...
%MULTINET-I-INSTALLING, Installing MultiNet base files
%VMSINSTAL-I-RESTORE, Restoring product save set F...
%MULTINET-I-INSTALLING, Installing MultiNet driver files
%VMSINSTAL-I-RESTORE, Restoring product save set G...
%VMSINSTAL-I-RESTORE, Restoring product save set I...
%MULTINET-I-INSTALLING, Installing MultiNet TCP/IP application files
%VMSINSTAL-I-RESTORE, Restoring product save set J...
%VMSINSTAL-I-RESTORE, Restoring product save set L...
%MULTINET-I-INSTALLING, Installing MultiNet NFS files
%VMSINSTAL-I-RESTORE, Restoring product save set M...
%VMSINSTAL-I-RESTORE, Restoring product save set O...
%MULTINET-I-INSTALLING, Installing MultiNet Secure/IP files
%VMSINSTAL-I-RESTORE, Restoring product save set P...
%MULTINET-I-INSTALLING, Installing the online documentation files
%VMSINSTAL-I-RESTORE, Restoring product save set Q...
%VMSINSTAL-I-RESTORE, Restoring product save set S...
%MULTINET-I-INSTALLING, Installing the include and library files
%MULTINET-I-INSTALLING, Installing the MultiNet HELP library
%MULTINET-I-MERGING, Merging SERVICES.MASTER_SERVER file
%MULTINET-I-DELETING, Deleting obsolete MultiNet files
%VMSINSTALL-I-MOVEFILES, Files will now be moved to their target
directories...
```

```
MultiNet Network Configuration Utility V4.3 (102)
[Reading in MAXIMUM configuration from MULTINET:MULTINET.EXE]
[Reading in configuration from MULTINET:NETWORK_DEVICES.CONFIGURATION]
[Writing Startup file MULTINET:START_MULTINET.COM]
Installation of MULTINET V4.3 completed at 12:30
Adding history entry in VMS$ROOT:[SYSUPD]VMSINSTAL.HISTORY
Creating installation data file: VMI$ROOT:[SYSUPD]MULTINET043.VMI_DATA
VMSINSTAL procedure done at 12:32
```

Note! Remember to reboot your system after upgrading the software.

Chapter 3

Files That May be Added to Your System Disk

The installation procedure may add the following symbiont files to the SYS$SYSTEM directory:

- MULTINET_LPD_SYMBIONT.EXE
- MULTINET_NTYSMB.EXE
- MULTINET_NW_PRINT_SYMBIONT.EXE
- MULTINET_SMTP_SYMBIONT.EXE
- MULTINET_STREAM_SYMBIONT.EXE

A data file for use with TCPVIEW is added as:

DECW$SYSTEM_DEFAULTS:MULTINET_TCPVIEW.DAT

The *Release Notes* are added as:

SYS$HELP:MULTINET043.RELEASE_NOTES

The MULTINET command is automatically added to:

SYS$COMMON:[SYSLIB]DCLTABLES.EXE

The MultiNet user commands may also be added to:

SYS$COMMON:[SYSLIB]DCLTABLES.EXE

The following shareable image may be added to SYS$LIBRARY:

MULTINET_LGISHR.EXE

Chapter 4

Removing MultiNet for OpenVMS

You can use the de-installation command procedure to remove the MultiNet for OpenVMS software. The procedure removes all MultiNet files from disk and all MultiNet commands from the DCLTABLES.EXE file. Before executing the procedure:

1	Use the LICENSE DISABLE or DELETE commands, or the VMSLICENSE command procedure to remove any registered MultiNet PAKs (Product Authorization Keys). If you are running MultiNet on a system running VAX/VMS V5.0 through V5.4, use the MULTINET:PAK-DELETE.COM procedure to delete the relevant PAKs. Refer to the Compaq Computer *VMS License Management Utility Manual* for more information about PAKs.
2	Remove the reference to START_MULTINET.COM from your system startup command procedure.
3	Remove system parameter changes in MODPARAMS.DAT made as part of the installation; invoke the AUTOGEN utility to set the parameters back to their pre-installation values. Refer to the Compaq Computer manual *Guide to Maintaining a VMS System* for descriptions of MODPARAMS.DAT and AUTOGEN parameters.
4	Reboot your system (or systems, if you installed MultiNet on more than one node in a VMScluster environment).

To execute the MultiNet de-installation procedure, type this command if MultiNet is still running:

```
$ @MULTINET:REMOVE
```

Otherwise, for V4.*n*-style installations, type:

```
$ @device:[directory.node.SYSCOMMON.MULTINET]REMOVE
```

device, *directory*, and *node* are those you specified during Step 8 of the installation procedure.

Or, for installations upgraded from MultiNet V3.*n*:

```
$ @target_volume:[SYSn.SYSCOMMON.MULTINET]REMOVE
```

See the MultiNet for OpenVMS V3.*n* documentation for the meaning of *target_volume* and **SYS***n*.

Chapter 5

MultiNet Documentation and Online Help

This chapter provides information about:

- The MultiNet documentation set
- Available online help for MultiNet

The MultiNet Documentation Set

The MultiNet documentation set consists of this guide and the following other publications:

MultiNet for OpenVMS Consolidated Release Notes	Describes new features in the software, known restrictions or problems, and corrections to the published MultiNet for OpenVMS documentation. Review the file SYS$HELP:MULTINET043.RELEASE_NOTES after installing the software. The same information is also available on CD-ROM distributions in PostScript format ([MULTINET043]MULTINET_RELEASE_NOTES.PS), in ASCII format ([MULTINET043]MULTINET_RELEASE_NOTES.TXT)
MultiNet for OpenVMS User's Guide	Explains how to explore your network, send and receive electronic mail, log into a remote system, transfer files between systems, and use DECwindows with MultiNet. Includes user command references.
MultiNet for OpenVMS Administrator's Guide	Explains how to configure and manage MultiNet.
MultiNet for OpenVMS Administrator's Reference	Identifies and describes MultiNet configuration and management commands.

MultiNet for OpenVMS Messages and Logicals Reference	Lists MultiNet messages and provides troubleshooting information as well as MultiNet logicals.
MultiNet for OpenVMS Programmer's Reference	Describes the MultiNet programming interfaces.
TCP/IP Services for DECnet Applications	Explains how to configure TCP/IP Services for DECnet Applications.

The following sections describe these documents in more detail.

User's Guide

Chapter 1 introduces the major topics and typographical conventions.

Exploring the Network

Chapter 2 introduces the network environment and covers the following topics:

- How to specify a remote host when using MultiNet commands
- Using the RUSERS command to determine who is logged in on your system, to your VMScluster environment, or at another site
- Using the WHOIS command to display information registered by the Internet NIC (Network Information Center) about your site, another site, or people associated with administering the network
- Using the FINGER command to display information about users
- Using the TALK command to contact other users over the network
- Using the REMIND command to post and receive reminder messages

Electronic Mail

Chapter 3 describes how to send and receive electronic mail across the network, and covers the following topics:

- Using OpenVMS mail to address network mail
- Using ALL-IN-1 or MailWorks

Kerberos Authentication

Chapter 4 describes the Kerberos authentication (security) system, and covers the following topics:

- Understanding how Kerberos works
- How to tell if Kerberos is available on your system
- Acquiring, deleting, and checking the status of Kerberos tickets that grant you permission to use various services
- Using Kerberos with the RCP, RLOGIN, RSHELL, and TELNET commands to gain access to remote hosts
- Changing your Kerberos password

Logging into Remote Systems

Chapter 5 describes how to log into and execute commands on remote systems, and covers the following topics:

- Logging into remote systems using the RLOGIN utility
- Executing commands on remote systems using the RSHELL utility
- Logging into remote systems using the TELNET utility

Accessing Files on Remote Hosts

Chapter 6 describes how to access files on remote systems, and covers the following topics:

- Using the RCP utility to copy files
- Using the TFTP utility to copy files
- Using the FTP utility to copy, rename, create, and delete files and directories

DECwindows and MultiNet

Chapter 7 describes general use of DECwindows with MultiNet, and covers the following topics:

- Requirements for running DECwindows applications over TCP/IP
- Authorizing remote systems to display windows on your local host

Secure Shell (SSH) Client

Chapter 8 describes how to configure and use the SSH client.

Appendix A describes the MultiNet user commands you can use from the DCL command line.

Appendix B describes the commands you can use during a session with the FTP file access utility.

Appendix C describes the commands you can use during a session with the TELNET remote login utility.

Appendix D describes the commands you can use during a session with the TFTP file access utility.

Administrator's Guide

This guide provides information about configuring and managing MultiNet.

Chapter 1 describes the organization of the guide.

Introduction to Configuration Tasks

Chapter 2 introduces configuration tasks. The major topics are:

- The task categories and the configuration methods available
- Starting MultiNet
- Modifying MultiNet configuration files
- Modifying the current configuration without restarting MultiNet

Establishing IP Connectivity

Chapter 3 explains how to establish IP connectivity between your system and other hosts on the

network, and covers the following topics:

- The meaning of IP connectivity
- An overview of interface configuration
- The supported network interface devices
- Viewing the current interface configuration
- Adding network interfaces
- Modifying and deleting existing network interfaces
- Understanding MultiNet Secure/IP
- Configuring IP-over-DECnet and IP-over-PSI
- Configuring SLIP (Serial Line IP) and PPP (Point-to-Point Protocol)
- Modifying global parameters that affect all network interfaces
- Configuring VMScluster aliases
- Making sure PATHWORKS support is enabled
- Enabling multicast packet reception
- Enabling and disabling MTU discovery

Configuring MultiNet Services

Chapter 4 describes how to configure MultiNet services, and covers the following topics:

- An overview of service configuration
- Configuring services with the command line server configuration utility, SERVER-CONFIG
- Using the SERVER-CONFIG commands
- Adding user-written services
- Disabling, enabling, and deleting services
- Configuring MultiNet Secure/IP
- Managing User Profiles and Programming Tokens
- Using MultiNet Secure/IP
- Using UCX-compatible services
- Specifying DCL command procedures as services
- Auditing and restricting access to services, files, and VMS processes
- Configuring services with the menu-driven configuration utility, MENU-CONFIG
- Configuring RLOGIN and RSHELL services
- Configuring the TELNET service for NTY devices
- Enabling and configuring SYSLOG message logging
- Enabling and configuring TFTP

Routing and ARP

Chapter 5 describes network routing, the ARP (Address Resolution Protocol) table, and GATED, and covers the following topics:

- MultiNet routing methods

- Configuring static routes
- Configuring router discovery
- Manipulating the ARP table
- Configuring GATED

Mapping IP Addresses and Hostnames

Chapter 6 describes host tables and DNS (Domain Name System) which are used to map between IP addresses to host names, and covers the following topics:

- An overview of methods for associating IP addresses with host names
- Using host tables
- Using DNS

Timezones and the System Clock

Chapter 7 describes how to specify timezones and synchronize your system clocks, and covers the following topics:

- Overview of the hardware clock and timezones
- Default and loadable timezone rules
- Using NTP (Network Time Protocol) time synchronization
- How to set hardware clocks on hosts not connected to the Internet
- Using the RDATE utility to set the local host clock by querying a remote system

Electronic Mail

Chapter 8 describes how to configure electronic mail, and covers the following topics:

- Modifying the MultiNet SMTP (Simple Mail Transfer Protocol) configuration file
- Configuring the SMTP server for inbound mail
- Configuring the SMTP symbiont and mail queues for outbound mail
- Delivering inbound mail to remote hosts via POP (Post Office Protocol)
- Configuring SMTP for ALL-IN-1 users
- Transferring mail between MultiNet and DECnet-only hosts

Printing Services

Chapter 9 describes the printing services provided by MultiNet, and covers the following topics:

- Configuring the LPD print service to allow other hosts and networks to access a printer
- Troubleshooting an LPD print server
- Configuring LPD and STREAM print queues
- Customizing print job processing with user exits
- Using the Network Terminal Symbiont (NTYSMB) for remote, network-connected printers
- Troubleshooting print queue problems

Remote Magnetic Tape and CD-ROM

Chapter 10 explains how to configure the RMT (Remote Magnetic Tape) service and how to use RMTALLOC (the RMT client) to create a device on your system that provides access to remote tape and CD-ROM drives. The topics covered are:

- Configuring the RMT service
- Configuring RMTALLOC

FTP Client and Server

Chapter 11 describes how to administer the FTP (File Transfer Protocol) client and server, and covers the following topics:

- Managing FTP clients
- FTP file name translation
- Managing the FTP service

RARP, BOOTP, and DHCP

Chapter 12 explains how to configure services to provide IP addresses and other configuration data for remote systems, and covers the following topics:

- Configuring RARP (Reverse Address Resolution Protocol)
- Configuring BOOTP (Bootstrap Protocol)
- Configuring DHCP (Dynamic Host Configuration Protocol)

Managing Hosts with XDM

Chapter 13 explains how to configure the MultiNet XDM (X Display Manager) server to manage remote hosts running X servers, and covers the following topics:

- How XDM provides login services
- Enabling XDM services
- Modifying the XDM configuration
- Controlling the XDM server (checking status, starting, stopping, restarting, and reloading the configuration)
- Controlling access to the XDM server
- Managing older X11R3 X Window System servers

Font Server

Chapter 14 explains how to use the MultiNet Font Server to provide fonts for X11R6 X Window Servers, and covers the following topics:

- Understanding the font server
- The font server configuration file
- Specifying the MultiNet font server
- Supported font types
- Enabling the font server

- Getting information about the font server
- Controlling the font server (starting, stopping, restarting, reloading the configuration, flushing the cache, and resetting)
- Defining font server catalogues
- Adding fonts to the font server

SNMP Agents

Chapter 15 explains how to configure an SNMP (Simple Network Management Protocol) agent, and covers the following topics:

- Understanding SNMP
- Configuring MultiNet SNMP services
- SNMP tasks using the MULTINET SET and SHOW commands

Secure Networks

Chapter 16 provides information about configuring and managing a secure network using Kerberos authentication services, and covers the following topics:

- Understanding Kerberos and the utilities used to create and maintain the Kerberos database
- Hardware requirements for the secure system
- Configuring Kerberos and testing the configuration
- Managing Kerberos
- Propagating the Kerberos database to other hosts

X11-Gateway

Chapter 17 describes the MultiNet X11-Gateway for X Window System connectivity between DECnet-only hosts and IP-only hosts, and covers the following topics:

- X11-Gateway concepts
- Configuring an IP client to access a DECnet server
- Configuring a DECnet client to access an IP server
- X11-Gateway security
- Debugging client-to-gateway connectivity

DECnet-over-IP Circuits

Chapter 18 describes DECnet-over-IP circuits, and covers the following topics:

- The tools for configuring DECnet-over-IP connections
- Examples showing how to connect two systems
- Improving performance
- Configuring DECnet devices for running DECnet over UDP

NFS (Network File System) Servers

Chapter 19 describes how to configure and maintain the MultiNet NFS Server software, and covers the following topics:

- Understanding the NFS Server software
- The tasks involved in configuring the NFS Server
- Enabling the MultiNet NFS Server
- Registering NFS Client users on your OpenVMS system
- Invoking the NFS configuration utility (NFS-CONFIG)
- Associating user names with UIDs and GIDs
- Exporting file systems to the network
- Reloading the NFS Server configuration and restarting the server
- Testing the NFS Server configuration
- Understanding NFS clients and configuring Sun workstation clients
- Restricting access to mount points
- Controlling NFS file access with access control lists
- Configuring PC-NFSD remote printing services for PCs and PC-compatible clients
- Booting diskless workstations with NFS
- Modifying NFS Server mount point options
- Understanding the global parameters that affect NFS Server operations
- NFS memory considerations
- Modifying the NFS Server file and directory cache
- Effect of the TIMEZONE parameter
- Special debugging parameters
- Troubleshooting

NFS (Network File System) Clients

Chapter 20 describes how to configure and maintain the MultiNet NFS Client software, and covers the following topics:

- Understanding the NFS Client software
- Basic NFS Client setup tasks (mapping UIDs and GIDs, reloading the NFS Client, and mounting file systems)
- Restrictions on using VMS BACKUP with NFS clients
- Advanced file system mounting options

Secure Shell (SSH) Server

Chapter 21 describes how to configure the Secure Shell server, and covers the following topics:

- Understanding the secure shell server
- Servers and Clients
- Security
- Options
- Configuration file
- RSA key file
- SSH daemon file

Service Parameters

Appendix A describes the service parameters you can set with the SERVER-CONFIG utility.

Administrator's Reference

This manual contains descriptions of all administrative commands:

- Commands you can run from the DCL prompt
- DECNET-CONFIG commands for configuring DECnet-over- IP circuits
- MAIL-CONFIG commands for configuring the SMTP mail system
- NET-CONFIG commands for configuring network interfaces and global parameters
- NFS-CONFIG commands for configuring NFS services
- NTYCP commands for configuring NTY devices for printing
- PRINTER-CONFIG commands for configuring remote print queues
- SERVER-CONFIG commands for configuring MultiNet services
- ACCESS-CONFIG commands for configuring MultiNet Secure/IP
- MultiNet Secure/IP DCL commands

Messages and Logicals Reference

This manual describes common messages encountered when running MultiNet, and covers the following topics:

- Verifying your configuration with the MULTINET CHECK and MULTINET X11DEBUG commands
- Getting more information about an error
- OpenVMS error values
- An alphabetical list of error messages
- Utility return codes
- UNIX error codes
- MultiNet logicals table

TCP/IP Services for DECnet Applications

This guide is for system managers who need to configure DECnet application services (formerly known as Phase/IP). This product lets applications designed for DECnet run over TCP/IP instead. This guide covers the following topics:

- Overview of DECnet application services
- Configuring, starting, and testing, including mapping DECnet names to TCP/IP domain names
- NOT-CONFIG commands for configuring DECnet application services

Programmer's Reference

This manual describes the MultiNet programming interfaces, and covers the following topics:

- Writing client and server applications

- MultiNet socket library functions
- The $QIO interface for more sophisticated programs
- Example application programs

MultiNet Online Help

MultiNet provides an extensive set of online help topics available at the DCL prompt:

```
$ HELP MULTINET
MULTINET
MULTINET is a set of commands for maintaining the MultiNet network.
Format
MULTINET  operation
Additional information available:

 Parameters Books  CHECK         CONFIGURE       DECODE       EMOSAIC

 FINGER            FONT          FTP             HOST_TABLE   KERBEROS

 LOAD              NFSDISMOUNT   Logical_Names   LPRM         NETCONTROL

 NETWARE           RCP           NFSMOUNT        NMP_Info     NSLOOKUP

 PING              PROFILE       RDATE           RFC_Info     REMIND

 RLOGIN            RMTALLOC      RSHELL          RUSERS       RWALL

 SEND              SET           SHOW            SKEY         TALK

 TCPDUMP           TCPVIEW       TELNET          TFTP         TOKEN

 TRACEROUTE        UNIX_Info     WHOIS           X11DEBUG     Programming
```

Chapter 6

Introduction to MultiNet and TCP/IP Concepts

This chapter presents a brief description of MultiNet and general concepts useful for understanding the MultiNet software and TCP/IP networking. This chapter describes:

- The MultiNet software for users, system managers, and programmers
- TCP/IP concepts, operation, and protocols, including:
  - Dynamic configuration protocols
  - Routing
  - DNS (Domain Name System) and host tables
  - ARP (Address Resolution Protocol)
  - SNMP (Simple Network Management Protocol)

Chapter 8 contains lists of books and RFCs (Requests for Comments) that provide more detailed information about TCP/IP.

What is MultiNet?

MultiNet is a collection of software that conforms to the set of internationally accepted standards for information exchange known as the TCP/IP protocol suite. The MultiNet software permits your VMS system to interact with other systems running TCP/IP software including PCs, Apple Macintosh systems, UNIX systems, and many others. Because TCP/IP is used on the Internet, using MultiNet lets you communicate locally, or globally with millions of other users and information services.

MultiNet provides applications, configuration tools, and programming libraries that make access to TCP/IP understandable and straight-forward. Whether your system serves one user or thousands of users, MultiNet gives all users access to a wide range of features that extend their use of the network and increase their productivity.

MultiNet works with the OpenVMS Operating System on the Compaq Computer VAX and Alpha architectures. On the VAX architecture, MultiNet works with VAX/VMS V5.0 and later and OpenVMS VAX V6.0 or later. On the Alpha architecture, MultiNet works with OpenVMS AXP V1.5 and later. MultiNet is distributed on CD-ROM, TK50 cartridge tapes, and 9-track magnetic tapes (VAX only).

MultiNet for Users

With MultiNet, users can:

- Send electronic mail to and receive electronic mail from other computer systems using SMTP extensions to OpenVMS Mail and ALL-IN-1 mail.
- Access the Internet and other information services.
- Log into remote systems using TELNET or RLOGIN.
- Execute commands on remote systems using RSHELL.
- Transfer files between local and remote systems with FTP, RCP, and TFTP.
- Print files and manage print jobs on remote systems with the LPD and LPRM utilities.
- Talk to other users interactively with the TALK utility.
- Display information about other sites and users with the FINGER, RUSERS, and WHOIS utilities.
- Read online information about MultiNet using either the DCL HELP facility.

MultiNet for System Managers

With MultiNet, system managers can:

- Configure devices and services easily with command line-based configuration utilities, or with the menu-driven MENU-CONFIG utility (MULTINET CONFIGURE /MENU).
- Provide IP connectivity for a variety of networking environments including IP-over-DECnet, Ethernet, FDDI, PPP, SLIP, and X.25.
- Provide other networking connectivity over IP, including DECnet-over-IP.
- Provide access to NFS-mounted file systems with the MultiNet NFS software.
- Change the current configuration dynamically by modifying logical name definitions or by using the NETCONTROL utility.
- Provide security for logging into systems across the network with Kerberos software.
- Create and access name servers with DNS (Domain Name System) software.
- Configure dynamic routing with the GATED service which supports routing protocols such as RIP, BGP, and others.
- Manage remote printing to print servers or to printers connected to the network with the LPD and stream client software.
- Provide remote access to local OpenVMS printers with the LPD server software.
- Provide electronic mail services with the SMTP and POP protocols; MultiNet provides SMTP enhancements for Message Router (MR), OpenVMS Mail, and ALL-IN-1.
- Access local and remote CD-ROMs, DATs, and conventional magnetic tape devices with the RMTALLOC utility.
- Synchronize system clocks from a central time server with NTP software and provide time updates to other hosts on the network.
- Provide binary compatibility with Compaq TCP/IP Services for OpenVMS (formerly called UCX) to support Compaq Computer and third-party applications such as TeamLinks, DECmcc, and applications written to use DCE for OpenVMS.

- Diagnose system problems and messages with the CHECK, PING, TCPDUMP, TCPVIEW, TRACEROUTE, and X11DEBUG utilities.
- View online information using either the DCL HELP facility.
- Access RFCs on the MultiNet CD-ROM consolidated distribution.

MultiNet for Programmers

With MultiNet, programmers can:

- Program with socket library routines.
- Work with a $QIO interface.
- Program with RPC library routines.
- Access sample programs and user exits that can be used to provide additional security and to customize other services (such as printing).
- View online information using either the DCL HELP facility.

TCP/IP Concepts

This section describes some of the basic concepts of TCP/IP networking.

Physical Networks

Physical networks are the cables and associated wiring components that link computers to one another for network communications. Common physical networks are Ethernet, Token Ring, FDDI (Fiber Distributed Data Interface), point-to-point links, and telephone with modems.

LAN (Local Area Network) Hardware Addresses

Network interface board manufacturers assign a unique hardware (physical) address to each interface board they produce. These hardware addresses are burned into the circuit at the time of manufacture, but can usually be overridden later by a network administrator, if desired.

A hardware address is usually composed of six numbers, one for each octet or eight-bit byte in the address value, separated by colons, such as 00:DD:A8:13:48:C5. The first three octets identify the manufacturer, while the remaining three octets are unique to the board.

Hardware addresses identify individual interfaces and aid in fast and efficient delivery of packets on the physical network.

IP Addresses

IP addresses identify hosts or interfaces on an IP network. An IP address consists of four numbers, one for each octet or eight-bit byte in the address value. IP addresses are written in dotted-decimal format, such as 191.87.34.22.

An IP address has two basic parts:

- A network number
- A host number

Traditionally, the portions of the address that identify the network and host were determined by the class of the network:

Class A networks	Class A addresses are identified by a value from 1 to 127 in the first octet, such as in 26.1.1.1. In class A addresses, the first octet identifies the network, while the three remaining octets identify the host. For example, IP address 26.1.1.1 identifies host 1.1.1 on network 26.
Class B networks	Class B addresses are identified by a value from 128 to 191 in the first octet, such as in 161.1.1.1. In class B addresses, the first and second octets identify the network, while the remaining two octets identify the host. For example, IP address 161.1.1.1 identifies host 1.1 on network 161.1.
Class C networks	Class C addresses are identified by a value from 192 to 223 in the first octet, such as in 197.1.1.1. In class C addresses, the first three octets identify the network, while the remaining octet identifies the host. For example, IP address 197.1.1.1 identifies host 1 on network 197.1.1.

With the introduction of subnet masks, the division between the network and host portions of an IP address has become much more flexible. See *Subnet Masks* for more information.

The network class determines the size of the network. A class A network can have 16,777,214 hosts, while a class B network can have 65,534 hosts, and a class C network can have only 254 hosts.

Subnet Masks

The original Internet addressing scheme made it possible for every host on a network to talk directly with every other host on the same network; other hosts were directly accessible if they used the same network number. In class A and class B networks, where very large numbers of hosts with the same network number are available, this scheme is no longer realistic because the underlying physical networks are constrained by bandwidth considerations. Ethernet and Token Ring networks cannot accommodate thousands or hundreds of thousands of hosts in a single, flat network space.

Subnet masks allow you to create multiple smaller networks from host addresses. For example, a class A network can be partitioned into class C subnetworks. These smaller, internal networks are called subnets. Subnet addresses are not exposed outside of the network; all changes to accommodate the additional addresses are handled internally. This simplifies routing information for the network and minimizes the amount of information the network must advertise externally.

Inside the network, you determine how to reallocate addresses by choosing how many bits of the host portion of each address are used as the subnet address and how many bits are used as the host address. You use subnet masks to divide the existing addresses into network and host portions. The subnet mask identifies how much of the existing address can be used as the network portion. The underlying physical network must also be divided into smaller, physical subnets when using a subnet mask to create subnets.

The following example illustrates how to create class C subnets from a class B network address:

The class B network address 161.44.0.0 can be divided by reallocating the first 24 bits of the 32-bit IP address to subnet addressing using the netmask 255.255.255.0. This reallocation allows you to use 161.44.1.0, 161.44.2.0, and so forth, up to 161.44.254.0 as network addresses. All traffic bound for any IP address beginning with the 16-bit network portion 161.44 will be routed to your site where internal routers handle subnetwork addresses. Valid addresses on the internal network, such as 161.44.4.42 and 161.44.224.12, can be reached from anywhere on the Internet; final delivery is handled by the routers on the individual physical subnets that contain the hosts associated with those addresses.

Broadcast Addresses

A system uses broadcast addresses to send information to all hosts on the network. Packets addressed to the network broadcast address are transmitted to every host with the same network number as the broadcast address. Broadcast packets are routinely used by the network to share routing information, field ARP requests, and send status and informational messages.

There are two common conventions used for broadcast addresses. The old convention, which older versions of SunOS and Berkeley UNIX BSD4.3 use, implements a broadcast address as the network portion of the address followed by all zeros. Using this convention, the broadcast address for the network 161.44 is 161.44.0.0. The new convention, which MultiNet and most other TCP/IP implementations use, implements a broadcast address as the network portion of the address followed by binary ones in all host portions of the address. In this scheme, the broadcast address for network 161.44 is 161.44.255.255.

If the network contains subnets, the broadcast address is relative to the local subnet. For example, host 128.44.12.1 with a subnet mask of 255.255.255.0 has an IP broadcast address of 128.44.12.255.

Host Names

Most sites assign host names to each system on the network because names are easier to remember than IP addresses. On a small, locally contained network, a host name may be only one word, such as WILLOW. However, on larger networks or on networks connected to the Internet, names are longer and denote a place in the organization and ultimately on the Internet. These longer, more detailed names are called fully qualified host names or fully qualified domain names (FQDNs). An example is WILLOW.FLOWERS.COM, where WILLOW is the individual host (or system) name, FLOWERS identifies the organization to which it belongs, and COM indicates this organization is involved in commerce on the Internet.

TCP/IP Operation

The following steps present a highly simplified view of the events that occur during successful network communication.

1	Using the appropriate application, such as electronic mail, a user initiates communication to another system, identifying the remote system by name, such as WILLOW.FLOWERS.COM.

2	The application asks for the IP address of the system identified as WILLOW.FLOWERS.COM.
3	Using either DNS or host tables, the IP address of WILLOW.FLOWERS.COM is determined.
4	A connection is established using a three-way handshake.
5	Application information is organized into packets for transmission across the network.
6	The MTU (Maximum Transmission Unit) of the physical network is determined; if necessary, the packets are fragmented before being sent to the network interface card for delivery.
7	The hardware address of the next host (or hop) in the route to the target host is determined.
8	Each host along the route receives the packets and forwards them to the next hop in the route.
9	Once the packets arrive at the destination, they are reassembled in the appropriate order and delivered to the appropriate application. Some protocols acknowledge receipt of the packets to the sending host.

Basic TCP/IP Protocols

Networking protocols ensure reliable delivery of information from one host to another.

This section describes several of the more important TCP/IP protocols.

- IP (Internet Protocol)
- TCP (Transmission Control Protocol)
- UDP (User Datagram Protocol)
- SLIP (Serial Line Internet Protocol)
- PPP (Point-to-Point Protocol)

IP (Internet Protocol)

IP (Internet Protocol) is the networking protocol used to deliver data packets from one computer to another. The computers may reside on different networks as long as information can travel between them.

The IP layer in a TCP/IP stack is responsible for:

Routing data packets from one system to the next until they reach their destination	When a packet is received, the IP layer examines its routing and interface tables to see if the IP address of the destination host is one of its own IP addresses or a broadcast address. If the destination IP address is the same as the local IP address, IP passes the packet to the TCP or UDP layer. If the IP address does not belong to this host and is not a broadcast address, the IP layer determines the next hop in the route. If this host is configured as a router, it forwards the packet to the next hop. If this host is not configured as a router, it discards the packet.
Discovering the MTU	The MTU (Maximum Transmission Unit) is the size of the largest packet that can be sent along the physical network. The MTU depends on the type of physical network being used. For example, a typical MTU for Ethernet networks is 1500 bytes, while a typical MTU for FDDI is 4352 bytes. When the IP layer receives a packet to send, it determines which route it will use to forward the packet and obtains that route's MTU.
Fragmenting and reassembling packets	If a packet is larger than the MTU, the IP layer is responsible for breaking the packet into smaller pieces or fragments that travel along the network. A fragment can be further fragmented as required by the next segment of the network. All reassembly occurs at the destination, where the IP layer is responsible for putting all the fragments together in the right order before passing the packets on to the TCP or UDP layer.

TCP (Transmission Control Protocol)

TCP (Transmission Control Protocol) provides a reliable mechanism for delivery of information to remote hosts.

On the sending host, the TCP layer of the TCP/IP stack is responsible for:

- Organizing the information sent by the application into segments (the amount of data that will fit into an IP datagram)
- Specifying the endpoints (ports) of the connection with the remote host
- Establishing a connection with the remote host
- Ensuring the remote host acknowledges packets that have been sent within a specified time

On the receiving host, the TCP layer of the TCP/IP stack is responsible for:

- Acknowledging received packets

- Organizing the packets into the correct sequence upon receipt from the sending host
- Forwarding the packets to the application using the specified port

TCP requires more overhead than UDP but provides reliable delivery of packets to the remote host.

UDP (User Datagram Protocol)

Applications can also use UDP (User Datagram Protocol) to deliver information to a remote host.

The UDP layer of the TCP/IP stack is responsible for:

- Organizing the information to be sent into a packet called a datagram
- Using a port to identify the program on the remote host to which the datagram is to be sent
- Verifying that the datagram contains the correct IP source and target addresses

UDP does not verify the successful delivery of packets to the target host. As a result, UDP requires less overhead than TCP. To accommodate this lack of verification, applications that use UDP often provide their own mechanisms for ensuring messages reach the target host in the correct sequence when required.

SLIP (Serial Line Internet Protocol)

SLIP (Serial Line Internet Protocol) allows the transmission of IP packets over serial lines. SLIP can be used over a direct connection between the serial ports of two systems, or over telephone lines with modems.

PPP (Point-to-Point Protocol)

Like SLIP, PPP (Point-to-Point Protocol) allows the transmission of IP packets over serial lines. PPP is a more versatile protocol than SLIP, and contains functionality that SLIP does not, such as:

- The ability to share the serial line with other protocols
- Error detection
- Support for both synchronous and asynchronous communication
- Dynamic configuration
- Negotiation of parameter values
- Support for different user-authentication protocols

While PPP is a more versatile serial-line protocol than SLIP, it is not available with all TCP/IP implementations.

Dynamic Configuration Protocols

To communicate with the rest of the network, a host must have an IP address. However, some systems do not have the hardware to permanently store an IP address. In addition, computers frequently share IP addresses when there are more computers than IP addresses, or when IP addresses are used only temporarily. For these situations, there are three dynamic configuration protocols: RARP, BOOTP, and DHCP.

RARP (Reverse Address Resolution Protocol)

RARP (Reverse Address Resolution Protocol) sends IP addresses to workstations that broadcast RARP requests containing their hardware addresses. RARP supplies IP addresses only and is commonly used by diskless workstations to determine their Internet addresses.

BOOTP (Bootstrap Protocol)

BOOTP (Bootstrap Protocol) lets a host receive an IP address and other configuration information from a BOOTP server on the network. BOOTP often specifies a bootstrap file for a client system to download, normally via TFTP (Trivial File Transfer Protocol). BOOTP lets systems that have no hard disk retrieve the information necessary to access their bootstrap file.

DHCP (Dynamic Host Configuration Protocol)

DHCP (Dynamic Host Configuration Protocol) builds upon the BOOTP protocol by letting a system receive all of the information necessary to function as a host on the network directly from a DHCP server. Unlike BOOTP, which only provides for permanent IP addresses, DHCP supports three different mechanisms for allocating IP addresses:

Automatic	Hosts requesting an IP address receive a permanent IP address
Dynamic	Hosts requesting an IP address receive a temporary IP address
Manual	IP addresses are manually configured and DHCP delivers the assigned addresses to requesting hosts

Routing

Routing is the process of selecting the path that data packets take to reach their destination. Routing can be as simple as delivering packets to another host on the same network (*direct routing*), or it may involve forwarding packets to routers on the way to the destination network. This section explains the basics of IP routing.

IP routing determines how to forward packets to a destination host. When a packet is forwarded to a local host (that is, a host on the same network), routing is *direct*; if the packet must be forwarded through one or more routers to reach its destination, the route is *indirect*.

Routing information for indirect routes is stored in a table of IP and router address pairs. Information in the routing table can be specified in three ways:

Static routes	Static routes are used to specify routing information explicitly. They are usually easy to maintain, but they provide no mechanism to respond automatically to changing environments.
Default routes	Default routes are used when a host has no specific route for the destination host or network in its routing table. If data cannot be delivered directly (because the routing table has no entry for the destination host or network), the data is forwarded to the default router.

Dynamic routing	Dynamic routing can use a service such as GATED to exchange routing information between cooperating systems. The protocols used to exchange information are RIP (Routing Information Protocol), EGP (Exterior Gateway Protocol), HELLO (DCN Local Network Protocol), and BGP (Border Gateway Protocol).

The following sections describe routing tables and GATED in more detail.

The Routing Table

The routing table stores information about the routes that hosts can use to reach other hosts on the network or Internet. The routing table entries can be configured statically by the system manager, or dynamically by a program such as GATED.

- Static entries are established by manually entering information. Once a static routing table is established, you must update the table as changes occur.
- Dynamic entries are generated from information provided by a routing protocol (such as RIP) which collects information from other routers to populate the table. Dynamic routing solutions automatically share information and update the table as routing information changes.

  The routing table is designed to supply the next hop address (which is always local) for data bound for other networks. The routing table never contains information about routers beyond the local network segment, nor does it contain information about how to reach individual host addresses (although it can contain host-specific entries). Routers always forward data to networks until the destination network is the local network. When the data arrives at the destination network, it is forwarded directly to the appropriate host.

  Host-specific routes are special routing table entries that specify which router to use when data is bound for a specific remote host. Host-specific routes are frequently used to test new routers or to implement network security procedures.

Router Discovery

Router discovery is a method of finding a router when no default route entry exists in the routing table. When booting, a host using router discovery broadcasts a message asking for available routers. The available routers reply with a message indicating their address. The host adds the information to its routing table and automatically sets the default route based on advertisements from routers on the local network. Local routers must also support RDISC (Router Discovery protocol).

GATED

GATED can both learn and advertise known routes, allowing for automatic handling of network configuration changes and automatic selection of the best available route. Other routers on the local network must also support at least one of the protocols used by GATED (EGP, BGP, RIP, and HELLO).

DNS (Domain Name System) and Host Tables

DNS (Domain Name System) and host tables are two methods of mapping between host (computer) names and their IP addresses. When you specify a host by name, DNS or host tables are used to map the host name to its IP address. The host name can be local to your organization or anywhere in the world, if your site is connected to the Internet. DNS and host tables can also be used to map IP addresses to host names.

DNS (Domain Name System)

TCP/IP applications use DNS to convert host names to IP addresses, and vice versa. This conversion is called resolving.

A DNS resolver sends requests to another computer, called a DNS server, to resolve names into IP addresses. The DNS resolver can also send requests to the DNS server to resolve IP addresses to names.

DNS servers store host name and IP address information. If your computer needs information that is not on one DNS server, the server automatically requests the information from other servers.

Domains

In DNS terminology, a domain is a group of computers. The domain administrator determines which computers are in the domain. A domain name identifies a domain and consists of words separated by dots. An example of a domain name is FLOWERS.COM.

The parts of a domain name are created by the domain administrator or may be special words used on the Internet. Domain names can pertain to a site, an organization, or to types of organizations.

When read right to left, the first word in the domain name is the top-level domain which identifies the function of an organization or specifies a country name code. In the name FLOWERS.COM, .COM indicates an organization engaged in commerce. The top-level domain can also indicate a country, such as .FR for France, or .IT for Italy. The name of the organization is to the left of the top-level domain, such as FLOWERS. Any words to the left of the top-level domain are called subdomains. The left-most word in the domain name is the host name. For example, in OAK.FLOWERS.COM, OAK is a host in the FLOWERS.COM organization.

Domains and subdomains are organized in a hierarchical tree structure. Just as the root directory in VMS is expressed as an implicit 000000., the root directory in DNS is expressed as a dot (.). Domains are analogous to directories; subdomains are analogous to subdirectories within directories.

Top-level domains such as .ORG, .COM, and .EDU exist in the United States. Other countries group their domain names below their two-letter country code. Domains grouped under country codes include domains such as .CO for commercial and .AC for academic. In the United States, .US is occasionally used instead of another top-level domain name. Subdomains may provide additional geographic information, such as .PALO-ALTO.CA.US.

DNS Server

A DNS server is any computer running DNS software that lets it communicate with other DNS servers and store address information for later retrieval. DNS servers are also called name servers.

Name servers cache (store) domain name information in memory for faster retrieval. Your network administrator provides the IP address of the name server on your network.

Hosts implementing DNS come in five varieties:

Root name server	A root name server provides information about the start or base of the domain name tree. A root name server delegates authority to other primary name servers for the top-level domains such as .COM, .EDU, .US, .IT, etc. A root name server usually also handles those domains just below the root.
Primary name server	A primary name server has authority over one or more domains or subdomains. A primary name server reads information about the domain over which it has authority from the zone file, a special file that describes information about the domain and the hosts in that domain.
Secondary name server	A secondary name server for a domain receives information updates from the primary name server for that domain at regular intervals, and stores this information on disk. A secondary server is also authoritative for the domain.
Caching-only name server	A caching-only name server is not authoritative for any domain. If a caching-only name server cannot resolve a request, it forwards the request to an authoritative name server for that domain and caches the results for future use.
Resolver	A resolver sends requests for resolution to a DNS server. Any name server that can handle the request returns the response.

Host Tables

If DNS is not configured on your network, you can configure MultiNet host tables to resolve names and addresses. Like DNS, host tables also map between IP addresses and host names; unlike DNS, however, the information is stored locally on your computer and must be updated manually. Using host tables, you must ensure that every host name you specify while running TCP/IP applications is listed with its IP address. Whenever a change occurs on the network, such as when a new computer is added that you need to access, you must add the information to the host table. With the growth of the Internet, maintaining host tables for it has become practically impossible.

When you add or modify a host table entry, you specify the host name, the IP address, an optional description, and one or more optional, alternative names (aliases) for the host.

Using DNS and Host Tables Together

If you are using DNS, you may also want to use host tables. This is useful for temporary situations, such as when a new computer is added to the network, but has not yet been added to DNS.

The advantage of using DNS and host tables together for name resolution is that your system can access other systems even if the DNS server is not running or if the network is down. If you

maintain entries in the host table for your local network, you can continue communicating with local systems until the DNS server or network is restored.

Warning!: It is crucial to keep your host table entries synchronized with the DNS information.

ARP (Address Resolution Protocol)

Before hosts can communicate with each other, the sending host must discover the hardware address of the receiving host.

Hardware addresses are unique numbers (for example, 00:DD:A8:13:48:C5) assigned to network interface boards by their manufacturers or by network administrators.

ARP (Address Resolution Protocol) discovers the hardware address corresponding to a specific IP address and dynamically binds the hardware address to the IP address.

ARP is a low-level protocol that lets network administrators assign IP addresses to hosts on a network as they see fit. There is no need to match the addresses to those on the physical network because ARP handles this process dynamically.

An ARP mapping (also called a *translation*) provides the correct delivery address (that is, the hardware address) on the network for data destined for an IP address. ARP mappings are stored in a table in memory known as the *ARP cache*.

When data is to be delivered to a local IP address (an IP address on the same physical network), the TCP/IP stack broadcasts an ARP request to all hosts on the local network segment. The request message asks all hosts if the IP address belongs to them. If the IP address belongs to a host on the local network segment, that host adds its hardware address to the packet and returns it to the sender. All other hosts on the network discard the request. The ARP cache stores the address resolution information returned and makes it available each time network data is bound for that IP address.

Old mappings are deleted from the ARP cache automatically after a short period of time. Old mappings are also deleted automatically when they no longer work (that is, when new, correct mappings become available).

SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) allows you to manage remote hosts on a network (for example, routers, hubs, and workstations). Both the network management host and the managed hosts (called agents) must follow the SNMP rules. Because SNMP is an open standard, you can mix and match network management hosts and agents from different vendors.

SNMP maintains information about your workstation in a management information base (MIB).

SNMP Traps

One of the main uses of SNMP is to make it easy to keep track of important events that occur on the managed network. To help automate network management, SNMP agents automatically send messages called traps to the network management host when certain events occur. For example, your workstation sends a trap when you reboot it.

One important type of SNMP trap is the *authentication failure trap*. Because SNMP network

management hosts have access to sensitive configuration settings for the hosts on a managed network, it is important for network administrators to guard against breaches in network security that involve illegitimate use of SNMP messages.

For this reason, every SNMP message must be authenticated by network management hosts and SNMP agents using passwords called *communities*. If your agent receives an SNMP message that contains an incorrect community name for the type of operation requested, your agent sends a message to a network management host. This message contains information about the request your agent received:

- What the message requested
- Why your agent would not fulfill the request

SNMP Communities

An SNMP community is a type of password used by the SNMP network management host and SNMP agents to ensure that only known and trusted hosts can send SNMP messages to and receive SNMP messages from each other. Every SNMP message includes a community name, so every message can be validated.

There are three types of community names:

Read	The network management host must use the correct read community name when asking your SNMP agent to send it information about your host.
Write	The network management host must use the correct write community name when asking your SNMP agent to change some characteristic about your configuration.
Trap	If certain events happen in your workstation (for example, when you reboot your host, or when a network management host sends an SNMP message that contains the wrong read or write community name), your SNMP agent sends a trap message to a network management host. If your trap message is to be handled, the trap community name you send must match the name known to the target network management host.

Chapter 7

Devices, Protocols, and MultiNet Internals

This chapter lists the devices and protocols supported by MultiNet and explains how the MultiNet kernel interacts with the OpenVMS Operating System.

Devices Supported by MultiNet

MultiNet supports a variety of network topologies. Table 7-1 lists the supported network interfaces.

Table 7-1 Supported Devices

Compaq Computer Ethernet controller (shared)
Compaq Computer FDDI controller (shared)
IP-over-DECnet link
IP-over-PSI link
Asynchronous PPP using any OpenVMS-supported terminal multiplexer
SLIP (Serial Line IP) using any OpenVMS-supported terminal multiplexer
Turbochannel and PCI Token-Ring interfaces for OpenVMS Alpha
Compaq Computer Token-Ring adaptors on OpenVMS Alpha

Protocols Supported by MultiNet

MultiNet is compatible with the current versions of the standard Internet networking protocol specifications listed in Table 7-2.

Table 7-2 Supported Protocols

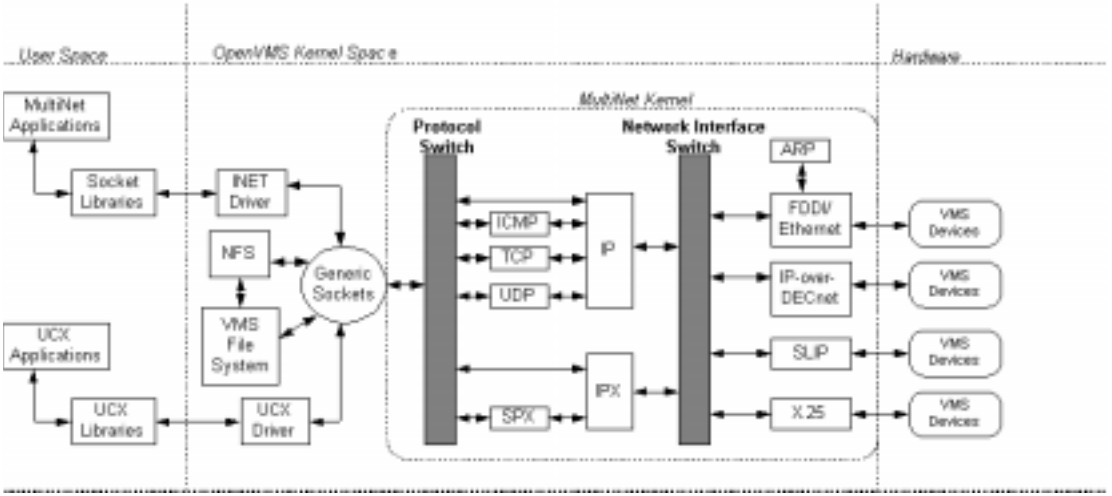
BGP (Border Gateway Protocol): RFC-1105, RFC-1323
BOOTP (Network Bootstrap Protocol): RFC-951, RFC-1534, RFC-1542, RFC-2132
DHCP (Dynamic Host Configuration Protocol):RFC-2131, RFC-2132
DNS (Domain Name Service): RFC-1034, RFC-1035, RFC-1101, RFC-1348
EGP (Exterior Gateway Protocol): RFC-904
Ethernet ARP (Address Resolution Protocol): RFC-826
Ethernet RARP (Reverse Address Resolution Protocol): RFC-903
FDDI (Fiber Distributed Data Interface): RFC-1188
FINGER (User Status Protocol): RFC-1288
FTP (File Transfer Protocol): RFC-959, RFC-1579
ICMP (Internet Control Message Protocol): RFC-792, RFC-1256
IP (Internet Protocol): RFC-791
IP-over-X.25: RFC-877
Kerberos: RFC-1411
NFS (Network File System): RFC-1094
NTP (Network Time Protocol): RFC-1059
Path MTU (Maximum Transmission Unit) Discovery: RFC-1191
POP2 (Post Office Protocol Version 2): RFC-937
POP3 (Post Office Protocol Version 3): RFC-1725
PPP (Point-to-Point Protocol): RFC-1332, RFC-1552, RFC-1661
RIP (Routing Information Protocol): RFC-1058
RPC (Remote Procedure Call Protocol): RFC-1057
SLIP (Serial Line Internet Protocol): RFC-1055, RFC-1144
SMTP (Simple Mail Transfer Protocol): RFC-821, RFC-822, RFC-974
SNMP (Simple Network Management Protocol): RFC-1157, RFC-1213
SYSTAT (Active Users Service Protocol): RFC-866
TCP (Transmission Control Protocol): RFC-793
TELNET (network virtual terminal protocol): RFC-854, RFC-855, RFC-856, RFC-857, RFC-858, RFC-859, RFC-860, RFC-885, RFC-1041, RFC-1073, RFC-1079, RFC-1091, RFC-1096, RFC-1205, RFC-1372, RFC-1411, RFC-1416
TFTP (Trivial File Transfer Protocol): RFC-1350
TN3270: RFC-1576
UDP (User Datagram Protocol): RFC-768
WHOIS (Directory Service Protocol): RFC-954
XDR (eXternal Data Representation): RFC-1014

Understanding MultiNet Internals

This section describes how the MultiNet kernel interacts with the OpenVMS Operating System. To understand the information in this section, some background in OpenVMS internals is helpful.

Figure 7-1 illustrates the MultiNet protocols and the overall organization of the MultiNet kernel.[1]

Figure 7-1 MultiNet Organization



MultiNet interacts directly with the OpenVMS Operating System. Generic sockets pass requests to the protocol switch, that differentiates between requests for IP use and for other support facilities. Requests are then sent through the network interface switch, which identifies the device for which the request is bound. When a request is received from a device, the steps occur in reverse.

The $QIO Interface

The programs implementing the lower layers of MultiNet—data link, network, and transport layers, with the exception of shared OpenVMS device drivers—reside in the MultiNet kernel. The MultiNet kernel is loaded into the OpenVMS S0 space (where the OpenVMS kernel is also loaded). Pages for S0 space are allocated when the OpenVMS system boots.

Note! You must use the SPTREQ SYSGEN parameter on VAX/VMS systems to set aside the appropriate number of S0 pages.

The MultiNet kernel accommodates multiple $QIO interfaces. Each $QIO interface is implemented by a separate OpenVMS pseudo-device driver, allowing MultiNet to simultaneously support the $QIO interfaces of several popular networking implementations. This lets you use, without modification, applications designed for these other networking implementations. The default MultiNet $QIO interface, implemented in INETDRIVER.EXE, is used by the MultiNet shareable socket library and all MultiNet applications.

All MultiNet $QIO drivers communicate with the MultiNet kernel through a set of kernel transfer vectors that interface with the generic socket layer. The generic socket layer of the MultiNet kernel

1. Support is provided for ATM, Ethernet, FDDI, and Token Ring as well as PPP and SLIP.

provides most of the facilities common to all network protocols (including reading and writing user-level data and synchronizing OpenVMS I/O request packets with network protocol events).

The generic socket layer uses the protocol switch for protocol-specific operations. The protocol-specific code (which may consist of several interconnected protocol modules) calls through the network interface switch to the appropriate network device driver to encapsulate and transmit packets.

The protocol-specific code can also receive timer interrupts through the protocol switch. Incoming packets are decapsulated by the network device drivers and passed to the protocol-specific code through the network interface switch.

Network Interface Device Drivers

The MultiNet kernel includes code allowing it to handle I/O for most network interface devices itself, rather than using OpenVMS device drivers. However, for devices that MultiNet shares with other software (for example, a Compaq Computer Ethernet interface), the kernel uses standard OpenVMS device drivers and either VCI (VMS Communication Interface), FFI (Fast Function Interface), or ALTSTART driver interfaces.

Custom Applications

The include and library files (optionally installed with MultiNet) provide access to several programming interfaces for writing custom client and server applications. These interfaces include:

- A 4.3BSD-compatible shareable socket library
- An RPC (Remote Procedure Call) library based on Sun Microsystems' public domain RPC library
- The standard MultiNet $QIO interface
- A $QIO interface compatible with the Novell[1] EXOS $QIO interface
- A $QIO interface compatible with the DEC TCP/IP Services for OpenVMS[2]

Consult the *Programmer's Reference* for additional information about the socket library and the MultiNet $QIO programming interface. The Sun RPC library routines are documented in the Sun Microsystems guide, *Networking on the Sun Workstation.* See the Novell guide, *LAN Service for OpenVMS TCP/IP Network Software Programming Guide* for further details about the Novell EXOS $QIO interface.

Table 7-3 shows the correspondence between the MultiNet components listed in Figure 7-1 and the layers of the OSI (Open Systems Interconnection) seven-layer reference model.

1. Formerly Excelan

2. Formerly called VMS/ULTRIX Connection or UCX (The Ultrix Connection). References in the MultiNet documentation set may refer to either UCX or DEC TCP/IP Services for OpenVMS.

Table 7-3 MultiNet Correspondence with the OSI Reference Model

Application, Presentation, Session	FTP, TELNET, FINGER, other applications
Session, Transport	TCP, UDP
Network	IP, ICMP
Data Link	Ethernet, ARP, X.25, IMP, 802.2
Physical	Coax, Fiber, Luminiferous Ether, and so on

Note! The protocol suites implemented under MultiNet do not map one-to-one onto the OSI reference model. In particular, each TCP/IP application protocol generally handles the functions normally ascribed to the Application and Presentation layers of the OSI model.

Chapter 8

Getting Additional Information

This chapter describes additional sources of information about topics relevant to MultiNet.

RFCs (Requests for Comment)

The Defense Data Network (DDN) Network Information Center (NIC) has collected extensive online archives of information useful to TCP/IP network designers and managers. Of particular interest are the Internet RFCs (Requests For Comments) that detail the protocol standards for the TCP/IP protocol suite.

The MultiNet consolidated distribution CD-ROM contains copies of the Internet RFCs in MULTINET:[CONTRIBUTED-SOFTWARE.RFC].

For a list of supported RFCs and information on obtaining them if your MultiNet distribution is on tape, invoke the following command:

```
$ HELP MULTINET RFC_INFO
```

Other Documentation

The following list describes additional documentation you can purchase about TCP/IP, UNIX, and other subjects relevant to an understanding of MultiNet. Read the FTP chapter of the *User's Guide* for instructions on accessing systems via anonymous FTP.

- *!%@:: A Directory of Electronic Mail Addressing and Networks*
  Donnalyn Frey and Rick Adams
  1989, O'Reilly & Associates, Inc., 103 Morris Street, Suite A, Sebastopol, CA 95472
- *DNS and BIND, Third Edition*
  Paul Albitz and Cricket Liu
  1998, O'Reilly & Associates, Inc., 103 Morris Street, Suite A, Sebastopol, CA 95472
  ISBN 1-56592-512-2
- *The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services*
  Ralph Droms and Ted Lemon
  1999, Macmillan Technical Publishing, 201 West 103rd Street, Indianapolis, IN 46290
  ISBN 1-57870-137-6

- *FYI on A Network Management Tool Catalog: Tools for Monitoring and Debugging TCP/IP Internets and Interconnected Devices, RFC-1470*
  IETF NOCTools Working Group
- *Handbook of Computer Communications Standards, Department of Defense (DOD) Protocol Standards, Volume 3*
  William Stallings, Paul Mockapetris, Sue McLeod, Tony Michel
  1988, Macmillan Publishing Co., New York, NY
- *Internetworking with TCP/IP, Volume I, Principles, Protocols, and Architecture, Internetworking with TCP/IP, Volume II, Design, Implementation, and Internals, Internetworking with TCP/IP, Volume III, Client - Server Programming and Applications*
  Douglas E. Comer (Volume I); Douglas E. Comer, David L. Stevens (Volumes II and III)
  Prentice Hall, Englewood Cliffs, NJ, ISBN 0-13- 468505-9 (Volume I), ISBN 0-13-472242-6 (Volume II), ISBN 0-13-47222-2 (Volume III)
- *Internet System Handbook*
  Daniel C. Lynch and Marshall T. Rose
  1993, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts
  ISBN 0-201-56741-5
- *Introduction to Administration of an Internet-based Local Network*
  Charles L. Hedrick
  Available via anonymous FTP from the host CS.RUTGERS.EDU in the "runet" directory. Available in both line printer format as the file "tcp-ip-admin.doc" and in PostScript format as the file "tcp-ip-admin.ps".
- *Introduction to the Internet Protocols*
  Charles L. Hedrick
  Available via anonymous FTP from the host CS.RUTGERS.EDU in the "runet" directory. Available in both line printer format as the file "tcp-ip-intro.doc" and in PostScript format as the file "tcp-ip-intro.ps".
- *Network Manager's Reading List: TCP/IP, UNIX, and Ethernet*
  Charles Spurgeon
  Available via anonymous FTP from the host FTP.UTEXAS.EDU in the "pub/netinfo/reading-list" directory. This list provides detailed descriptions of each book and categorizes documents by skill level. The reading list is available in both line printer format as the file "net-read.txt" and in PostScript format as the file "net-read.ps". Accessing systems via Anonymous FTP is described in detail in the FTP chapter of the User's Guide.
- *Site Security Handbook, RFC1244*
  P. Holbrook, J. Reynolds
  1991
- *TCP/IP and NFS, Internetworking in a UNIX Environment*
  Michael Santifaller
  1991, Addison-Wesley Publishing Company, Wokingham, England
  ISBN 0-201-54432-6
- *TCP/IP For Dummies—A Reference for the Rest of Us!*
  Marshall Wilensky and Candace Leiden
  1995, ISBN 1-56884-241-4 IDG Books Worldwide, Inc.,
  An International Data Group Company,

919 East Hillsdale Blvd., Suite 400, Foster City, CA 94404

- *TCP/IP Illustrated, Volume I: The Protocols*
  W. Richard Stevens
  Addison-Wesley Publishing Company, Reading, Massachusetts,
  ISBN 0-201-63346-9
- *TCP/IP Illustrated, Volume II: The Implementation*
  W. Richard Stevens, Gary R. Wright
  Addison-Wesley Publishing Company, Reading, Massachusetts,
  ISBN 0-201-63354-X
- *TCP/IP Network Administration*
  Craig Hunt
  1992, O'Reilly & Associates, Inc.,
  103 Morris Street, Suite A, Sebastopol, CA 95472
- *The Hitchhiker's Guide to the Internet, RFC-1118*
  Ed Krol
- *The Internet Companion, A Beginner's Guide to Global Networking*
  Tracy LaQuey with Jeanne C. Ryer
  Foreword by Vice-President Al Gore
  1993, Addison-Wesley Publishing Company, Inc., Reading, Massachusetts
- *The Matrix: Computer Networks and Conferencing Systems Worldwide*
  John S. Quarterman
  1989, Compaq Press, Bedford, Massachusetts
- *The Simple Book, An Introduction to Management of TCP/IP-Based Internets*
  Marshall T. Rose
  1991, Prentice Hall, Englewood Cliffs, NJ,
  ISBN 0-13-812611-9.
  Describes SNMP (Simple Network Management Protocol)
- *There's Gold in Them Thar Networks! Or Searching for Treasure in all the Wrong Places, RFC-1290*
  J. Martin
  1991, Ohio State University, available by anonymous FTP from DS.INTERNIC.NET in the rfc directory as the rfc1290.txt file. This document lists many sources of information about the Internet and TCP/IP available from other anonymous FTP sites.
- *The Whole Internet User's Guide & Catalog*
  Ed Krol
  1992, O'Reilly & Associates, Inc., 103 Morris Street, Suite A, Sebastopol, CA 95472
- *UNIX Network Programming*
  W. Richard Stevens
  1990, Prentice Hall, Englewood Cliffs, NJ,
  ISBN 0-13-949876-1
- *Users' Directory of Computer Networks*
  Tracy L. LaQuey
  1990, Compaq Press, Bedford, Massachusetts
- *Writing Real Programs in DCL*

Paul C. Anagnostopoulos
1989, Compaq Press, Bedford, MA,
ISBN 1-55558-023-8.
This document provides information about writing VMS command procedures.

- *X Window System, The Complete Reference to Xlib, X Protocol, ICCCM, XLFD*
  Robert W. Scheifler and James Gettys
  1992, Compaq Press; order number EY-J802E-DP
- *X Window System Administrator's Guide*
  Linda Mui and Eric Pearce
  Volume Eight of the O'Reilly X Window System series,
  O'Reilly & Associates, Inc.,
  ISBN 0-937175-83-8
- *Zen and the Art of Internet, A Beginner's Guide*
  Brendan P. Kehoe
  1992, PTR Prentice Hall, Englewood Cliffs, New Jersey,
  ISBN 0-13-010778-6

Index

X

Reader's Comments
MultiNet for OpenVMS Version 4.3 Installation and Introduction, Part Number: N-5004-43-NN-A

Your comments and suggestions will help us to improve the quality of our future documentation. Please note that this form is for comments on documentation only.

I rate this guide's:	**Excellent**	**Good**	**Fair**	**Poor**
Accuracy	o	o	o	o
Completeness (enough information)	o	o	o	o
Clarity (easy to understand)	o	o	o	o
Organization (structure of subject matter)	o	o	o	o
Figures (useful)	o	o	o	o
Index (ability to find topic)	o	o	o	o
Ease of use	o	o	o	o

1. I would like to see more/less:_____

2. Does this guide provide the information you need to perform daily tasks?_____

3. What I like best about this guide:_____

4. What I like least about this guide:_____

5. Do you like this guide's binding? If not, what would you prefer?_____

My additional comments or suggestions for improving this guide:_____
_____

I found the following errors in this guide:

Page	**Description**
_____	_____
_____	_____

Please indicate the type of user/reader that you most nearly represent:

System Manager	o	Educator/Trainer	o
Experienced Programmer	o	Sales	o
Novice Programmer	o	Scientist/Engineer	o
Computer Operator	o	Software Support	o
Administrative Support	o	Other (please specify)	o _____

Name:_____ Dept._____
Company:_____ Date_____
Mailing Address:_____

After filling out this form, FAX or mail it to:
Process Software, 959 Concord Street, Framingham, MA 01701-4682
Attention: Technical Publications Group FAX 508-879-0042 e-mail:techpubs@process.com